MP 180672
MITRE PRODUCT

MITRE

Essential Considerations for Actionable Analysis

Project No.: 10AOH810-JF

Lexington Park, MD

Author:

F. Lynam

Peer Review:

R. Ligon
B. Race
L. Oringer
R. McInnes
M. McFarren
A. McEachron
J. Kressel
C. Jantsch

October 2019

Abstract

This paper outlines basic design of analysis concepts, particularly bounding and conservatism. These concepts are used to differentiate types of analysis, and when each should be applied. This paper is intended for analysts who want to understand basic ideas in design of analysis. This paper argues that systems-engineering efforts of substantive weight (in terms of cost, public safety or national security) have a responsibility to provide formal evidence of bounding and conservatism in the design of their analysis.

Overview

The management of programs and operations requires continuously making well-informed decisions. When selecting a strategy to execute or solution to employ, some understanding of how likely the selected option will be to achieve the desired outcome, particularly with respect to other alternatives, is required. Analysis is the mechanism used to develop that understanding.

In matters of significant weight in terms of cost, public safety or national security, analysts have a responsibility to provide formal, credible evidence to substantiate their conclusions. For matters without strong theoretical underpinning to shape such analysis, test data provides the initial basis to develop a novel formal understanding of knowable elements of a problem. This paper provides key concepts for how to differentiate types of problems and how to characterize the relationships between analysis, testing, and decision-making in a manner that enables the determination of what can be considered credible evidence.

Modes of Information-Constrained Decision-Making

Decisions are made to either obtain a desired outcome or to avoid an undesirable one. Often, we have too little information at the time of a decision to truly demonstrate the probability of obtaining either of those conditions, or to fully explore all possibilities. Thus, decisions are usually made with some degree of confidence using incomplete information, and this uncertainty about the outcome needs to be handled differently depending on the consequences of being wrong.

Self-knowledge about incomplete information has been described using a model that divides the universe into three essential elements: things we know (**known knowns**), things we know we don't know (**known unknowns**), and things we don't know we don't know (**unknown unknowns**). For example, we may know the results of a virus scan (known knowns), and we may know that vulnerabilities can exist that won't be detected by that scan (known unknowns) but we may fail to consider that the virus scanning tool could be lying to us about the scan results (unknown unknowns).[1]

System Models and Conservatism

We have high confidence in precise values for known knowns. We have low confidence and wide uncertainty about known unknowns. We have no data about unknown unknowns. We must account for each accordingly.

When optimizing for desirable outcomes, we generally have to pick one option out of many. We can describe the set of all possible choices as a space full of options, where we can reach in and pick any one that satisfies our needs. In some cases, we may be so fortunate as to have options available that are likely to succeed built entirely from known knowns. This means not only are those options likely to succeed, but we also have a high confidence that that estimation of success is highly accurate. However, when we must rely on some known unknowns, we may have less confidence in that prediction, even if

[1] Luft, J.; Ingham, H. (1955). "The Johari window, a graphic model of interpersonal awareness". Proceedings of the western training laboratory in group development. Los Angeles: University of California, Los Angeles.

we estimate success is likely. The mean expected value might be the same, but the span of where reality might actually lay is much wider.

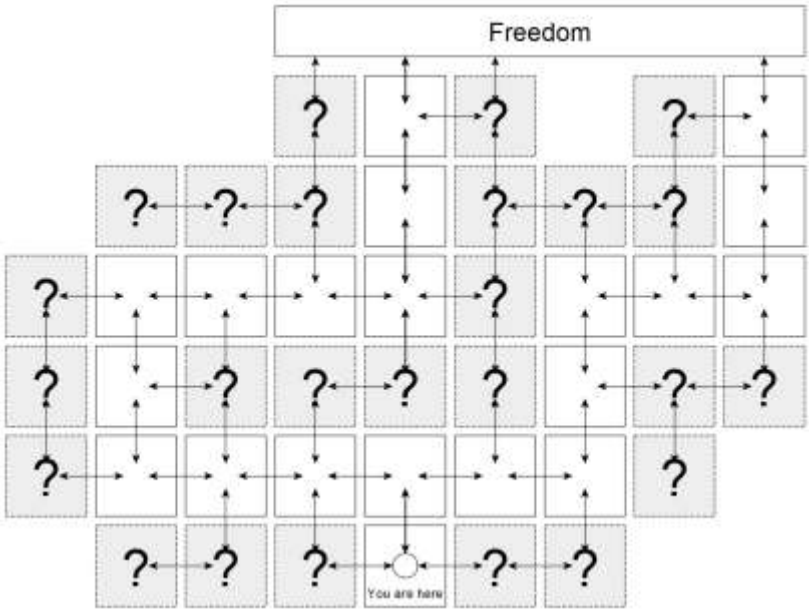

Figure 1 - Two Paths Through a Large Facility of Interlocking Rooms

Imagine we are thieves in a large facility full of interlocking rooms. We just stole the crown jewels, tripping the alarm, and need to get out of the facility before the police arrive. Our set of escape options are all the paths through the facility, but we only know a few rooms well, and we can guess at a few immediately adjacent to those with less confidence. To pick our path, however, we only need to know one route that meets our decision criteria: one acceptable, high confidence option out of the space of all possible solutions, one path that we can trust with certainty. Even if we don't understand anything about the rest of the facility except that path, we can have a high confidence of successfully escaping. For all the doors we pass, each one could lead to an exit or a guard, and we won't know. The **conservative** choice – i.e., the choice that minimizes the possibility of failure – is therefore to follow the path we know is safe and fast.[2] If we have low confidence that a door is an exit, we shouldn't take it.

In contrast, when optimizing to avoid undesirable outcomes, our confidence about the rest of the information outside the known knowns starts to strongly shape our acceptable solutions. Undesirable outcomes can precipitate even from unknown unknowns. We consequently need to invest in an understanding our own level of understanding in order to make informed decisions, to help us understand the space of all possible problems.

In the facility example, imagine that now we are the guards, planning how to prevent future thefts. But in this imaginary scenario, our facility is so theoretically large and complex that even we don't have the map of the whole facility. In real operational defensive scenarios, in the field or in cyber space, this can often be the reality to varying degrees: we have systemic uncertainty about what we're defending, and finite resources to information gather. For the thief, the set of all possible escape paths were an

[2] National Academy of Engineering (US). Hazards: Technology and Fairness. Washington (DC): National Academies Press (US); 1986. Dealing With Uncertainty About Risk in Risk Management.

uncertain solution space extraneous to the one good option, but for us defenders they become an uncertain problem space that must be addressed.

Assume we have one mitigation: locking the doors. They're big, complicated locks, and it takes us some amount of time to secure each one. The alarm just tripped, and the thief is escaping with the crown jewels, so we don't have time to lock them all. We know it takes the thief some amount of time to pick each lock, so our solution-space is now notionally defined by some set of doors we should lock in the time available to provide the most confidence that as many paths, or "problems," have been addressed as possible.

If we are confident a particular door leads to an escape, we should certainly lock it. But what if we don't know where a door leads and don't have the extra time to expend on finding out? Just like the thief, for us that door could lead to an exit or another guard. But when making decisions to avoid an undesirable outcome, we defenders now treat that uncertainty differently: if we have low confidence that a door isn't an exit, we should lock it.

Interaction-Models and Bounding

The secure facility example above illustrates how the question being answered changes how we conservatively manage and bound uncertainty in analysis. How we respond to uncertainty when optimizing for likelihood of success changes depending on whether success means finding one path through the facility or stopping all paths. Obtaining a specific desirable outcome may be best assured by ignoring very likely solutions with a high uncertainty of success, like shortcuts that might contain guards. Avoiding a large problem space of undesirable outcomes may be best assured by investing in unlikely problems when we lack confidence in our predictions, like locking doors that might lead to nowhere.

Our analysis involves the relationship between two conceptual models: the adjacency of various rooms (system model), and the nature of that adjacency (interaction model). What if our interaction model of the system is wrong? Imagine there are actually three ways to traverse between rooms: opening unlocked doors, picking locked doors, and using a chainsaw to cut through walls. We know about the first two: it is a known known that opening an unlocked door takes very little time, and the time required to pick a lock is a known unknown, which means it falls in some uncertain range of possible times. But if our model of movement between rooms only includes doors and lock picks, then the chainsaw is an unknown unknown: something we haven't accounted for.

This completeness of the model for interactions in a system limits the ability of the overall system model to be complete. When the interaction model is incomplete, the conclusions must be considered **not bounding**: they do not exhaustively describe the problem space. Systematic error is introduced when we fail to account for an unknown unknown such as chainsaws, and consequently we are not presenting an accurate picture of the risk of someone else finding a way through the facility. We may fail to make the best possible decisions to prevent that outcome, or there may be more residual risk than we estimate.[3]

A bounding interaction model is about more than creating predictions based on previously collected data. For example, there is no evidence that the standard model of physics itself is some fundamental

[3] Greenland, S. (2004). "Bounding Analysis as an Inadequately Specified Methodology". Risk Analysis, Vol. 24, No. 5. Invited Commentary.

truth: it is simply a theoretical description of relationships that is highly consistent with a tremendous amount of data. That consistency does not eliminate the possibility of creating a new, completely different model that has a lower margin of error than the current model, nor the possibility that all physics experiments in all of history are merely random noise. Those possibilities are simply unlikely. However, every subtle complexity and dependency in the standard model of physics was carefully selected, incorporated and substantiated by observable evidence: any interaction model requires both a compelling theoretical basis and sufficient evidence to support the complexity of all necessary assumptions. These theoretical models that we use to describe the way reality works build on each other as we collect more data. We came up with an explanation for gravity that mostly worked for the data we had, then figured out ways to tweak it for edge cases over and over until we got to the standard model of physics. Each new complexity was earned along the way through arduous labor.

The Null Hypothesis of Risk

Statistics provides a tool to estimate hypothetical situations by using past data about real situations. The statistical process for estimating confidence in an outcome that is the focus here involves demonstrating that the distribution of probable values for one hypothetic situation, the "null hypothesis," is different than the distribution of probable values for a different hypothetic situation, the "alternative hypothesis." Normally this is done by showing that the two distributions overlap less than some defined confidence value. For example, by showing that the distribution of probable values for "time for the thief to escape the facility" is less than the distribution of possible values for "time for the police to show up."

Figure 2

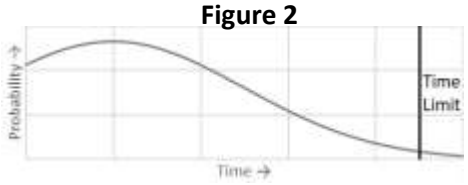

Figure 2 illustrates just such a case. Here, the null hypothesis is that the time to escape exceeds an upper limit defined by "when the police show up." This null hypothesis may often be very well known and is shown here as a very narrow distribution. In this case, escape times that fall to the left of the black Time Limit line are acceptable to us, and those to the right are not. However, the time required to escape may be more poorly known and have some large possible range. The curve shows a distribution of the possible times it could take to escape.

In this illustration, only a small fraction of possible times exceeds the acceptable limit, approximately 0.1%. In the shown example, the "time to escape" and "time when the police arrive" curves are clearly different. In fact, we are able to reject the null hypothesis at the 99.9% confidence level (sometimes written as "p = 0.001"). If we are a very risk-averse thief, perhaps we would use a minimum acceptable confidence of "rejecting the null hypothesis" (getting caught before our escape) as a criterion for selecting targets. That would be an excellent method to manage the risk of capture.

Being able to demonstrate that a single solution is viable requires confidence on one hypothesis, in this case that we can escape in time. Being able to demonstrate that no problems exist is fundamentally different, however, and requires confidence in two sets of values: the estimate for every predictable problem, and the estimate for how much of reality is covered by our definition of the problem space.

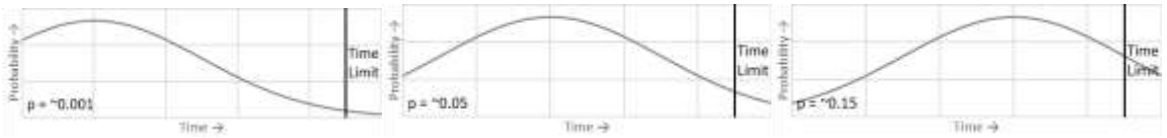

Figure 3

The objective of hypothesis-testing in this decision-making case is to be able to claim that most of the escape routes (probable time distributions for three different routes are illustrated in Figure 3) are longer than it takes for the police to arrive to some large degree of confidence.

If we combine all of the possible routes into a single plot, every path can be qualitatively described based on its relation to our time limit and what our acceptance criteria for residual risk is:

Figure 4

Imagine, mirroring the thief, the guards want to *deter* thieves to a 99.9% confidence, such that thieves would compute that only 0.1% of their probable escape times will be before the police arrive. Our baseline facility contained paths acceptable to even the most risk averse thieves, paths with a 99.9% confidence of being below the limit. Some other paths may have been so long to already meet our criteria, having a 99.9% confidence of the time required to follow them exceeding the time limit. But some paths are likely in-between, with more than 0.1% of the probably times falling longer than the time limit, but also less than 99.9% of them. If we wanted to deter only the very risk-averse thieves, we would only need to fix paths with a 99.9% confidence of being shorter than the time limit. But we want to deter even the foolhardiest of thieves, so we must treat the presence of all of those in-between cases as unacceptable as well.

This approach doesn't handle unknown unknowns, however. To do that, we need to estimate how much of the possible space of problems or solutions is covered by our set of predictions. This is a different kind of acceptance criterion that didn't matter to our thief: maximum allowed systemic error. Given sufficient data about representative past heists, we can measure our confidence that we are predicting all possibilities in our interaction model, and that we've credibly bounded the set of all possible paths in our problem space. Then, using that interaction model to define the possible permutations of escape routes, we can now measure our confidence in covering all of the paths. A bounding model is one that can provide evidence to substantiate the hypothesis that the contribution of all unknown unknowns in the interaction model and system model, the maximum systemic error, is expected to keep residual risk within acceptable limits.

Modes of Analysis

Analysis methods can be generally described in relation to their ability to manage the issue illustrated in Figure 4, which relates directly to which type of information constraints dominate our knowledge of the decision space: unknown unknowns, known unknowns or known knowns. Further, depending on the mode of decision making, obtaining a desired outcome or avoiding an undesired outcome, we must handle this center region differently.

Figure 5

When known knowns dominate the problem space, as in Figure 5, we have a very good understanding of the problem. The confidence in the completeness and coverage of the interaction model is very high (unknown unknowns are small), and the uncertainty in predictions from our interaction model is very low (known unknowns are small). As a result, the distributions for predicted outcomes in the system model are very narrow around an estimated mean, resulting in little chance to overlap the threshold value. This means that the space in the center of Figure 5 is relatively small: we are able to confidently assert whether a particular system model outcome falls to the left or the right of our threshold value. Regardless of the mode of decision making, the decision is clear for each result.

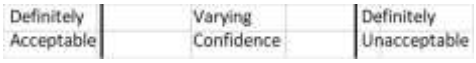

Figure 6

When known unknowns dominate the problem space, as in Figure 6, we have a high confidence in the completeness and coverage of the interaction model (unknown unknowns are still small), but now we have a low confidence in the particular predicted values. This creates wide distributions in the system model which often overlap the threshold value, and a large central region where results have varying degrees of confidence. This results in a unique situation, where often we are not able to confidently characterize whether a particular outcome is below the threshold or above it.

Figure 7 illustrates how the mode of decision making, obtaining or avoiding, becomes significant to the treatment of this region of varying confidence. When attempting to obtain a desired outcome, it is conservative to reject the central region from the solution space as the confidence of the desired outcome is below the acceptance criteria. When attempting to avoid an undesired outcome, it is conservative to include the central region within the problem space, as the confidence of avoiding the desired outcome is now below the acceptance criteria.

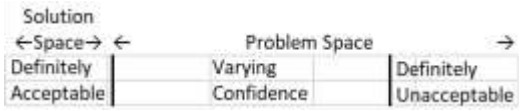

Figure 7

For example, imagine that we performed an analysis on our model which gives us confidence that 95% of all expected interactions fall within the model parameters: “unlocked doors and lockpicks” bounds 95% of movement between rooms, as only 5% of thieves ever think of using a chainsaw. Now, we perform our system model analysis which shows us that all possibilities within the problem space are within a 90% confidence interval: all possible paths through the facility are conservatively longer than the threshold and unacceptable for someone else to attempt. We would now have a 95% confidence that 90% of outcomes are managed within acceptable limits.

Unbounded Problems

When a problem is poorly defined and there is low or no quantifiable certainty in the completeness of the interaction model for a system, then the decision space is not bounded by the analysis. This means that both solutions and problems may exist that cannot be predicted by the interaction model describing the system – unknown unknowns. For example, a facility interaction model lacking chainsaws

cutting through walls may fail to describe escape paths which involve walls with no doors. Testing, past data and empirical evidence are valuable tools to start building the foundation of knowable elements of a problem in order to estimate confidence in the ability of a model to bound a problem and substantiate credible conclusions.

Problems that are poorly understood or defined can lack an effective means to consistently characterize empirical data early on in data collection. Consequently, these problems are often dominated by best practices and heavily driven by subject matter expertise: informal methods that effectively attempt to intuit a consistent theoretical model of the system without demonstrating consistency of that model empirically. In lieu of using an empirical basis, subject matter expert judgement is relied upon with no tie to substantiating evidence.

Such informal treatment of problems presents significant risk to misleading the decision-making process by instilling overconfidence in the effectiveness of a proposed course of action, particularly when presented from a position of technical authority. When a problem space is not well bounded, the limitations of the presented solutions must be very clearly articulated to the decision maker. Good engineering judgement must be employed to continuously question the credibility of any analysis to acceptably bound risk to a degree sufficient to warrant any proposed action.

Error and Risk Acceptance

Characterizing residual uncertainty, the conceptual “error bounds” on a result, is critical in conveying risk to decision makers. Sources of uncertainty in analysis which may include in their error adverse results pose risks that decision makers must be aware of when using that analysis to make a decision. If the analyst fails to take adequate precaution to manage and communicate sources of error in the analysis process, decision makers are unwittingly taking on risks that they have not explicitly considered, and in effect the analyst is accepting that risk on their behalf.

Conservatism in analysis is one means to mitigate the possibility of such unanticipated risks. An appropriate level of conservatism can facilitate more rapid results by avoiding complex problem spaces, allowing for timely decision making, which is in itself often a meaningful risk reduction. However, over-conservatism with respect to poorly understood problems can waste resources unnecessarily. Investment in an appropriate level of analysis is a critical consideration in the execution of analysis.

When known unknown dimensions dominate a problem space, intentional conservatism provides more confidence that no risks are realized by simplifying to a minimum viable analysis product. This has the adverse effects of rank reversal between alternatives and potential determination of an inability of any feasible alternative to meet requisite acceptable residual risk. For example, consider constructing a bridge. In this simplified example, we can build either a wood or steel bridge, based on whether the minimum cost of a bridge with a specific load bearing capacity fits within an available budget. Here, only the cost and the load bearing capacity of the bridge are being used to inform the decision.

If we had perfect knowledge of the strength and cost of the materials, that knowledge might tell us that both bridges meet acceptable strength at acceptable cost, with steel being the cheaper option. However, we rarely have perfect knowledge. If our knowledge of the strength of steel has a great deal of uncertainty, the conservative, risk-adverse option is to assume that the strength of steel is on the weak end of the uncertainty range. This over-conservative margin of safety on the strength of steel could then

result in the determination that the cost of an acceptable steel bridge exceeds the cost of the wooden bridge, reversing the rank preference.

Where many uncertainties are large, the effect of conservatism on rank reversal is simply a natural impact of that uncertainty: the analysis cannot demonstrate a particular rank preference with meaningful confidence. Our best guess from the information we have might be not to go with the steel.

Often analysis is performed on very small amounts of data. Where there is little data, uncertainty is high. As a consequence, conservative analysis with high uncertainty can result in the conclusion that there are no options within cost constraints. However, when faced with high uncertainties and no clear options, it is reasonable to invest instead in reconsidering the conservative or bounding assumptions within the model and performing a more detailed analysis. Collecting more data or analyzing more dimensions of the problem can potentially buy back margin not by changing the system, but by reducing the known conservative bias and error in the analysis conclusions. Here, “sharpening the pencil” through additional modeling fidelity or test data could reduce those uncertainties and demonstrate an acceptable option exists. We might discover that the strength of steel is on the high end of our range.

When problems are sufficiently well known that these issues can be avoided, such as in highly mature fields like strengths of materials and bridge construction, known known effects dominate. The scope of problem space with variable confidence is highly diminished in these cases, as well as the impact of handling that space of varying confidence very conservatively.

The appropriate use of conservatism in an analysis depends on the impact of the accepted risks, and the process of defining conservative minimum acceptance criteria can be challenging. For manufacturing, the impact of error can be explicitly quantified in the economic consequence of delivering defective equipment. However, for analyses involving strategic national security or large-scale public health risks, the impact of residual risks can be extremely high, and acceptance criteria applied to manufacturing or the sciences may not be appropriate.

For such analyses which may entail exceptionally grave impact to national security or the public, conservatism in the treatment of uncertainty is a necessity. Decision makers must drive risk as low as reasonably achievable by continuously improving analysis, mitigating risks, balancing the costs of analysis and mitigation and always leveraging good engineering judgement to question the completeness of the underlying models. Further, in these situations, a failure to provide design and operational margin to accommodate systemic uncertainty with respect to unbounded risks poses a uniquely great danger. Selecting a course of action in the absence of an empirically-sound understanding of the problem, such as by performing non-conservative risk analysis or without leaving additional robustness for unknown unknowns, has the potential to silently accept significant risks.

Conclusion

Analytic understanding of problems evolves over time through the continued collection of empirical data, from an unknown unknown dominated space, to a known unknown dominated space, and eventually to a known known dominated space. The application of analysis must adapt to provide appropriate handling of problems in each of these spaces. It is the responsibility of the analyst to use good engineering judgement in the conservative and bounding application of data to accurately convey risks in support of well-informed decision making.