Perspectives on Managing Risks in Energy Systems

Richard Kim[a], Tina Diao[b], and Madison Coots[c]
[a] Aerospace Technical Services, Palo Alto, CA, richard.kim@aerospacetechnical.com
[b] Aerospace Technical Services, Palo Alto, CA, tina.diao@aerospacetechnical.com
[c] Aerospace Technical Services, Palo Alto, CA, madison.coots@aerospacetechnical.com

Abstract: Modern enterprise risk management (ERM) for complex engineered systems is ultimately concerned with making high-quality resource allocation decisions at the organizational level with the goal of minimizing the risk of these systems. Effective ERM is challenging in several ways: 1) it necessitates the continuous monitoring and assessment of a comprehensive set of risks; 2) it requires a cogent measure of value and objectives; and 3) it requires a normative decision framework that is grounded in quantitative measures, rather than heuristics. In this paper, we describe a principled approach for ERM to address these pressing challenges in complex systems across numerous industries but with a focus on energy systems. We begin by outlining and explaining the methods comprising the Risk Management Toolkit: a set of rigorously tested quantitative methods with a proven track record for bolstering the efficacy of modern ERM programs. We then outline a set of organizational characteristics that we believe play instrumental roles in ensuring effective ERM across an organization. Finally, we use an illustrative example system from the energy sector to perform an economic analysis of the organizational value of an effective ERM team. Ultimately, our analysis underscores the significant value and importance of employing thoughtful and rigorous methods of risk management, and our results generalize naturally to other industries with similarly consequential systems.

1. INTRODUCTION

Energy infrastructure is of national significance and is closely intertwined with a country's economic power [1]. When poorly built or maintained, these systems may not only severely hinder economic growth, but they may also cause financial and societal setbacks. In recent years, energy systems have experienced several such setbacks in the form of high-profile failures that resulted in property damage and lives lost. For example, in November 2018, California experienced its deadliest wildfire in history: the Camp Fire. The Camp Fire resulted in 85 fatalities, $16.65 billion in assessed property damage, and displaced 52,000 residents. Investigators later found that a likely cause of the fire was a failed c-hook on a transmission tower, resulting in a wildfire-causing ignition [2]. On June 16, 2020, PG&E pleaded guilty to 84 counts of involuntary manslaughter for those who died in the Camp Fire [3]. Without proper interventions, the consequences from such natural disasters are expected to be more severe as human-caused climate change is compounded with increasing housing density [4].

The Camp Fire example illustrates both the importance of employing effective enterprise risk management (ERM) in energy systems, as well as the significant negative consequences associated with the mismanagement of risk. Inadequate institutional risk management processes rendered decision makers unable to make the management decisions required for mitigating the risk of catastrophic outcomes. Innovations in ERM that enable risk managers to more effectively manage and mitigate such risks are therefore vital to the progress and long-term survival of organizations in the energy sector.

ERM is a strategic approach to consider, in a coordinated manner, all sources of risk present in the enterprise's value chain [5] and to make resource allocation decisions to increase the expected value measure of a principal objective [6]. Effective ERM is fundamentally a high-quality decision-making process that yields clear and actionable recommendations to stakeholders. Ultimately, this process optimizes enterprise-level tradeoffs amongst attributes that include quantified opportunities, losses, as well as costs in both the short- and long-terms.

It is challenging for energy systems to conduct ERM effectively for several reasons. First, effective ERM requires a comprehensive assessment of all sources of risk [7]. Facing multiple uncertainties simultaneously, organizations have typically taken a more siloed approach to performing risk assessments by analyzing financial, environmental, reputational, legal, safety, and other risks separately, but rarely taking a unified approach to analyzing these risks in tandem and at the enterprise level [8]. Second, the objective of ERM is commonly profit maximization, which is often measured by the creation of wealth for shareholders. Unfortunately, maximizing profit is not always perfectly aligned with minimizing risks to health, safety, and environment (HSE), and minimizing the occurrence of integrity incidents [9]. As a result, organizations may be faced with the task of managing competing objectives. Third, there is oftentimes a lack of a normative decision-making framework for ERM. A normative decision-making framework discourages the approach of addressing risk on a decentralized basis and instead roots itself in well-established methods of organizing decisions, uncertainties, and values into a unified, coherent model. In the absence of such a framework for ERM, executive leadership and corporate boards are often forced to make investment decisions based upon heuristics, nullifying any systematic risk analysis that may have been performed. Fourth, modern ERM requires a higher-skilled workforce that is not only well-versed in the specific domain—in energy systems, for example—but is also trained in extracting insights from data for the use of effective decision making.

This article seeks to outline the necessary components of achieving effective ERM with examples from energy systems. Despite the focus on the energy sector, however, the underlying principles generalize to other sectors that involve the management of complex and consequential systems. The following sections are organized as follows: in Section 2, we discuss the legacy methods of risk management, which continue to be widely used by risk groups, despite their inadequacies; in Section 3, we explain and motivate the use of the Risk Management Toolkit, an ensemble of risk management tools; Section 4 summarizes the complementary managerial aspects of ERM; and in Section 5, we provide an economic analysis that demonstrates the economic benefits of employing thoughtful and principled ERM.

Throughout our discussion of the Risk Management Toolkit in Section 3, we will provide examples of a real-world risk management activity that we performed for a mid-tier California investor-owned utility. To maintain client privacy, we will refer to this organization as Cal Utility Corp.

2. LEGACY RISK MANAGEMENT METHODS AND THEIR WEAKNESSES

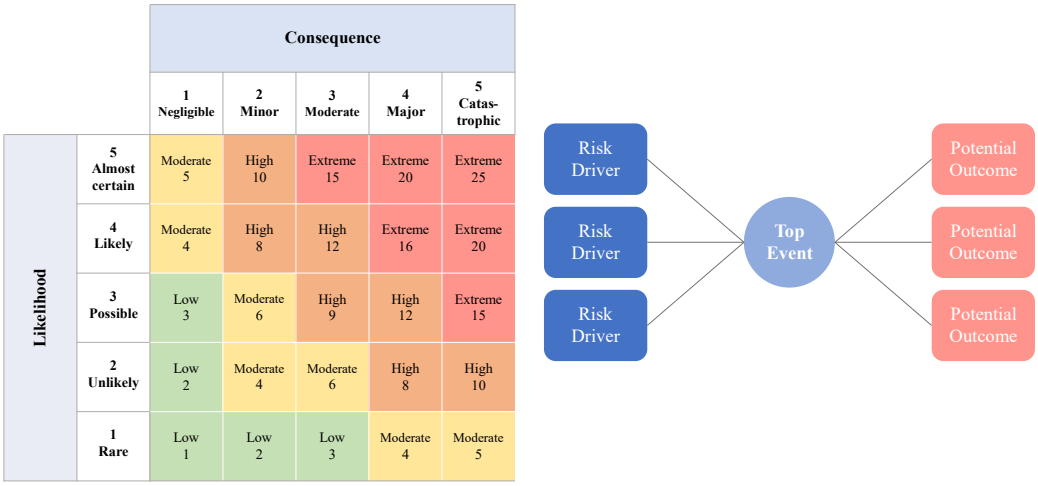
The first step towards effective ERM is the adoption of rigorous assessment methods for the various risks an organization may be exposed to. The criterion of rigor—quantitative or qualitative—must consistently consider all facets of the risks examined without excluding possible risk interactions or making flawed assumptions that may potentially lead to adverse consequences. However, many legacy risk management methods rely heavily on heuristics and frameworks that often oversimplify the risk landscape and fail to capture critical interactions between risks. In the sections below, we briefly describe two of the most common legacy methods that are still used in practice today.

2.1. Risk Matrices

The risk matrix, depicted in Figure 1 (left) [10], is a highly qualitative method of depicting relative severities among a set of known risks. While the risk matrix is still widely today, it is not recommended as a component of ERM for several reasons. First, risk matrices exhibit a lack of clarity in how measures such as likelihood and consequence are defined. As a result, these quantities are subject to variable interpretation by different stakeholders. Second, likelihood and consequence bins all have the same relative scale, which may not be appropriate when comparing different classes of risks. For instance, a 1% chance of human fatality and 1% chance of computer server failure have significantly different impacts on risk management, and yet would have the same “rare” likelihood rating on the risk matrix. Third, risk matrices do not depict dependencies between risks. Discrete dots on the risk matrix depict independent risk events, however, many risks are probabilistically dependent. It is possible that two

"low" risks that are dependent on one another could occur simultaneously, resulting in a "severe" risk event. Such interactions cannot easily be captured and tracked in the risk matrix. Fourth, risk matrices do not adequately depict how risks change over time. Instead, they provide a static view that represents risk as single snapshots in time. Finally, the categories within risk matrices cannot be directly used to make decisions on resource spending, which is a primary purpose of any risk assessment method [11].

Figure 1. (Left) Example of the classic 5x5 risk matrix. (Right) Example of the risk bowtie.



2.2. Risk Bowties

The risk bowtie, depicted in Figure 1 (right) [12], represents a marginal improvement from the risk matrix because it attempts to structure risks as a sequence of drivers and outcomes. It proposes a way to use data to quantify risk and potentially provides clearer action in terms of resource allocation decisions with respect to the identified risk drivers.

However, the risk bowtie also has significant shortcomings. First, standards on risk management via bowties [13] dictate the use of frequencies to describe driver likelihoods [14]. Analysts should avoid using frequencies and instead use probabilities and probability distributions for the occurrence of risk driver events. When frequencies are utilized, distribution information is condensed into a single point value and the underlying distribution cannot be recovered. In contrast, probability distributions are much more informative, allowing for risk operators to make inferences on the probabilities of additional adverse events. Second, risk bowties inherently make assumptions on the causal relationships between risk drivers and risk outcomes. In practice, it is impossible to fully justify causal effects between a finite set of drivers and a finite set of outcomes, while still guaranteeing that causal effects are not assumed erroneously or missed altogether. By establishing this logical tautology, strong claims of causality are made with no justification and these assumptions can lead to incorrect risk analysis results. Finally, risk bowties are difficult to utilize when one is interested in a highly granular examination of an engineered system because the bowtie does not enable a systems decomposition process.

While these qualitative methods of describing and assessing risks are suboptimal and inappropriate for the reasons described previously, they are still used widely throughout many sectors. For instance, in their 2018 Safety Model Assessment Proceeding (S-MAP), the California Public Utilities Commission (CPUC) stipulated a risk-based decision-making framework that is grounded in the use of risk bowties [13]. In response to this regulatory mandate, PG&E developed a risk bowtie showing the loss of containment on a gas transmission pipeline listing drivers such as third-party damage and stress corrosion cracking. The outcomes included events such as pipeline ruptures and leaks [15]. While the bowtie incorporates the likelihood and consequence of risk events of the listed known events, it is unlikely that the bowtie method would identify a driver that has not been seen before (when its historical frequency is zero) and/or not assumed a priori to be causal to the loss of containment. Similarly, it is

unlikely that the risk bowtie method, when applied to the public utility's wildfire risk, would have identified the c-clamp that caused the Camp Fire in advance of its failure [16].

3. THE RISK MANAGEMENT TOOLKIT

Organizations that have recognized the limitations of legacy risk management models have adopted a wide variety of methods that enable more effective risk management, resulting in reduced risk costs from operations. This section aims to explore these modern methods that enable the highest quality of risk management. We will refer to this collection of methods as the Risk Management Toolkit. Together, these tools represent insightful applications of well-studied methods from probability theory, optimization, and stochastic modeling. As such, they afford the analyst a rich set of tools that can be used to analyze a system rigorously and thoroughly. Ultimately, we claim that the adoption of the Risk Management Toolkit is instrumental for achieving high-performance enterprise risk management.

To further motivate our discussion of the Risk Management Toolkit, we will also present several examples of applications of these methods from a real project performed for Cal Utility Corp. In 2020, Cal Utility Corp was interested in better understanding the risk of unintentional wildfire ignitions from its transmission towers. We performed an in-depth risk analysis of an archetypical transmission tower that ultimately yielded several valuable risk insights, including the baseline probability of ignition from the structure, the set of components that contributed the most risk to the system, and recommendations for the most optimal risk mitigations to invest in (considering both cost and risk reduction value). Throughout this section, we will describe how we leveraged methods from the Risk Management Toolkit to produce these insights and recommendations for Cal Utility Corp. It is worth noting again that, while this case study aimed to characterize the risk of an energy system, the Risk Management Toolkit is industry-agnostic and can readily be applied to any engineered system.

3.1. Decision Analysis

The ultimate purpose of any risk analysis is to serve as a decision support tool for human decision makers. Hence, the overarching analytical basis for risk management must be based on a normative decision analytic framework, using well-established methods such as von Neumann Morgenstern utility theory. Given key uncertainties and objective values (typically in units of dollars), decision analysis allows decision makers to evaluate multiple alternatives for risk management, while also factoring the risk attitude of the decision maker. As such, decision analysis provides executive leadership a mathematical certification of optimality in their decisions, which minimizes common cognitive biases such as anchoring, recency, and the availability bias [17].

To use decision analysis in conjunction with multi-attribute value functions, one encodes the utility associated with the different attributes—for example, the statistical value of life, the value of lost electric service, the value of structures destroyed—into a single numerical value with no units attached to it [18]. Values of each attribute are compressed into a single number representing that set of attribute values for the attributes considered. For example, for the set of example attributes listed previously, the conversion would accept three numerical inputs—one value for each attribute—and then produce a single number. The conversion is based on a set of weights that capture the relative value of changing the outcome of each attribute dimension from its worst possible value to its best possible value. The single multi-attribute value is simply the weighted sum of the values reported for each attribute.

To explicitly model the risk preference of a decision maker, one can employ a nonlinear functional form of a utility curve, such as the exponential transformation of native dollars into utility (or disutility, as appropriate). The use of utility theory with encoded risk attitude is well-established and widely adopted in applications of decision analysis to financial and human safety risks, particularly those pertaining to energy systems. For example, Brito et al. [19] assesses operational risks associated with natural gas pipelines using a multi-attribute utility model that includes human, environmental, and financial risks. The risk model applies a classic exponential utility function to encode risk preference. Cha and

Ellingwood [20] examine nuclear regulatory decision-making (in the United States and other nations) and observe differing levels of risk aversion in different regulatory regimes.

3.2. Value of Information (VoI) Analysis

The value of information refers to the change in expected utility that a decision maker would experience as a result of having additional information regarding a key relevant uncertainty at the time a decision is made. Effectively, a VoI analysis answers the question: “Is it worth it to obtain additional information?” While this concept stems directly from the fundamentals of decision analysis, we feel that it warrants its own discussion due to the essential role it plays in ERM. The primary premise behind VoI is that all information comes at a cost and not all information is worth acquiring when making a decision. Examples of information pertinent to ERM include results from parts inspection, additional parts testing, or expert opinions.

Additional information serves to improve a decision maker’s state of knowledge on risks only if pursuing this information outweighs the cost of obtaining it. The additional benefit from marginal information is computed by looking at the difference between two quantities. The first is the cost to the decision maker from having acquired additional information, and the second quantity is the new expected utility associated with having the additional information, which can be computed using the decision analysis framework described previously. If the difference between the marginal benefit and cost values is positive, then the additional information is worth acquiring, up to a cost that equals the difference; otherwise, it is not. In some instances, VoI computations show that the cost of information-gathering efforts, such as increased parts inspections, is greater than the value returned as a result of the additional information. In such cases, the VoI analysis suggests that such efforts are to be avoided, oftentimes in opposition to the intuition of decision makers.

3.3. Probabilistic Risk Analysis (PRA)

Probabilistic risk analysis (PRA) is a framework for functionally decomposing engineered systems and identifying the sources of risk present within the system. Grounded in applications of methods from probability theory, PRA assesses complex engineered systems from a distinct systems engineering perspective by decomposing systems into their components and then using Bayesian networks to infer system-level failure modes and failure probabilities. The output of a PRA consists of the system’s probability of failure, the system’s potential root causes of failure and their associated probabilities of occurrence, as well as an absolute risk ordering of system components.

PRA has its roots in a seminal paper written by Dr. Allin Cornell in 1968 entitled "Engineering Seismic Risk Analysis" [21]. Dr. Cornell’s paper laid the foundations for quantitative risk analysis by developing methods to assess seismic risk. This paper was immediately used to improve upon legacy methods of risk analysis in the early years of the transition from the nuclear navy to civil nuclear power generation. In subsequent decades, PRA has been applied to petroleum systems [22], aircraft systems [23], civil infrastructure projects [24], as well as healthcare systems [25].

During the risk analysis project for Cal Utility Corp, we utilized PRA to perform a functional decomposition of an archetypical transmission tower to understand how individual components worked in tandem to support the overall function of the tower. Using these insights, we utilized PRA, for which one of the first analytic steps is the construction of the fault tree of the system. Intuitively, a fault tree is a graphical tool that encodes the Boolean logic that describes how functions or components of a system relate to possible failure modes of the system. The fault tree is therefore what enables an analyst to compute the comprehensive set of failure modes for the system. In the context of the Cal Utility Corp project, system failure was defined to be unintentional ignitions from the tower, potentially leading to wildfires.

Following the computation of the overall probability of failure of the system along with root failure modes and their probabilities, an analysis of individual component importance factors (such as Fussell-

Vesely Importance) suggested that the highest risk components were the connection points between large mass components in the tower such as the tower lattice structure and conductors, as well as connection points that bear long-term low-grade stress such as hooks, clamps, and splices. This finding was validated by the utility's field operators who have observed the greatest wear on components such as hooks and clamps, particularly in high wind regions of California.

3.4. Loads and Capacities Analysis

Many engineering contexts require a different modeling approach, treating both the system's capacity and the potential load as sources of uncertainty. An example of such a system is a gas pipeline, where the pipeline's true capacity is unknown (despite its specifications), and the load experienced by the pipeline fluctuates stochastically according to consumer demand. Considering loads and capacities together is sometimes referred to as statistical interference, because their overlapping probability distributions resemble interfering signals. Ultimately, all risks can be characterized as systems with uncertain design capacity experiencing uncertain loads. In a probabilistic framework, these uncertainties can be modeled as probability distributions with overlapping probability density functions (PDFs). These PDFs can further be utilized to identify components which are most susceptible to the risk of overloading failure. The output of this analysis informs decision makers of the probability of component and system failure, given knowledge of the stochastics present in the system.

In 2010, a gas pipeline owned and operated by Pacific Gas & Electric (PG&E) in San Bruno, CA exploded, causing eight fatalities and destroying thirty-eight homes [26]. The 2012 CPUC incident report [27] on this catastrophic event revealed that one of the root causes of the explosion was PG&E's failure to consider cyclic fatigue [28] or other loading conditions while practicing "spiking" to meet increased customer demand for natural gas. While the report refers to cyclic fatigue as "an unknown threat," the possibility of catastrophic failure due to the pipeline bearing excessive load is a classic example of overloading failure risk, and this risk could and should have been identified using loads and capacities analysis.

3.5. Resource Optimization

With a convex optimization framework, it is possible to compute optimal resource allocation policies that describe how marginal dollars should be spread across the system—in the form of risk mitigation measures, such as reinforcement, redundancies, and enhanced inspections—to maximally mitigate risk. The output of a resource optimization analysis is a policy table that, given different budgets, describes the optimal allocation for spreading marginal risk mitigation resources to maximally reduce the system's overall probability of failure.

In our analysis of Cal Utility Corp's transmission tower system, an accompanying analysis involved the development of an optimization model that provided the optimal policy for spreading marginal risk mitigation dollars across system components via reinforcement, replacement, or more frequent inspection. We performed an analysis of historical maintenance records along with data elicitation sessions with their subject matter experts to derive convex investment-failure response curves at the component level. These data were then aggregated to derive a system-level response curve, which provided a convex region amenable for optimization. We then minimized a system-specific form of an objective function that represented that system's baseline probability of failure as a function of investments in individual components in the system. We constrained the sum of the investments to equal the total budget (as specified by the stakeholders) and constrained the investment in each component to be non-negative. The result of solving this optimization problem was a policy for how marginal dollars should be spread across components (such as hooks, clamps, and conductors) to maximally reduce the system's probability of failure.

3.6. Optimized Inspection Policies

In a resource-constrained operational environment, system inspections should be prioritized in a manner where inspection resources are directed to yield the greatest prophylactic benefit against risks. For instance, an electric transmission system that adheres to a blanket inspection policy, such as "fully inspect the system every five years by inspecting a non-overlapping 20 percent portion of the system each year" is wasteful. This is because components across systems have a highly heterogeneous mix of risk profiles. For example, a component in a gas distribution system that is newly installed will presumably have a lower level of failure risk, and therefore should have a lower inspection priority, than a component that was installed 30 years ago and was last inspected five years ago. By modeling physical component deterioration over time using available data, a prioritization framework can be built to optimally assign priorities to parts with the greatest failure risk. Inspection policy computations can utilize discrete state space, finite time Markov chains to identify the components that are at greatest risk of failure prior to inspections. Markov chains accomplish this by characterizing the probabilities of transitioning from one state of operations to another, which can then be used to infer steady state probabilities. For example, the state of health for a component in a system can be classified as new, minor fault, major fault, or failed. Data can then be analyzed to determine the probabilities that the component will transition from one state to another, which can then be used to infer the steady state probability that the component will be in a failed state. If this probability exceeds a given tolerance threshold, decision makers may take corrective action. Ultimately, this analysis informs decision makers on how to direct limited inspection resources to obtain maximal efficacy.

3.7. Optimal Recapitalization Policies

In risk management of large, complex systems, there exists a class of management decisions that are recurrent with high periodicity. A classic example is the optimal recapitalization of components to minimize failure risk, where components are under continuous review or high frequency periodic review. These recurrent recapitalization decisions typically take the form of the question: "When should we replace or reinforce components that may soon fail?" From the operations management perspective of complex systems, it is useful to consider that there exist opposing forces on cost. On one hand, systems face the risk of unplanned downtime due to parts failure. On the other hand, excessive reinforcement or parts redundancies impose excessive costs from overengineering. Therefore, optimal recapitalization policies should be computed by finding a local minimum of combined costs (failure risk costs plus operational management costs). A proven method utilized for this analysis is a form of dynamic programming called Markov decision processes (MDP) [29]. This method models a time-variant sequential decision-making process that outputs a time-*invariant* optimal policy table that informs decision makers of the actions which result in optimal risk reduction of the system.

3.8. Data Analysis

The efficacy of mathematical models is limited by the quality of its input data. Risk models are dependent on data-informed inferences on component states of health and probabilities of failure, and effective data analysis can enable higher quality analyses of system risk. Ultimately, effective data analysis capabilities enable the decision maker to extract hidden wisdom from the data to inform quantitative risk management models. For example, in a separate recent effort with Cal Utility Corp, the client was interested in a closer examination of the use of Public Safety Power Shutoffs (PSPSs). The decision of when and where to invoke PSPSs is preceded by a significant amount of deliberation due to the potential adverse outcomes associated with either alternative. The decision to enact a PSPS is accompanied by economic costs associated with disruption of service to consumers, whereas the decision to forego a PSPS may be accompanied by costs associated with catastrophic wildfires that may have been prevented by a PSPS.

Cal Utility Corp has long had a decision support tool for evaluating PSPS decisions. This model utilized static conditions, based upon historical distributions of wind speed to determine when current conditions exceed a predefined percentile threshold on the historical distribution, thus triggering a PSPS. The utility sought to improve upon the static model by building a "dynamic" PSPS model, which utilized additional data sources, along with near real-time data on weather conditions to more judiciously utilize

PSPS to mitigate wildfire risk. While their efforts are still in their nascent stages, it is clear that there is still much work to be done in order to maximally extract knowledge from the large volumes of available data to build effective decision support models. This requires trained personnel who understand the methods of data science, including the suite of algorithms under the umbrella of machine learning. Furthermore, expertise in detection theory could be leveraged to combine the signals from both the static and dynamic PSPS models to improve the decision making regarding when and how to use PSPSs.

4. CHARACTERISTICS OF EFFECTIVE ENTERPRISE RISK MANAGEMENT

The methods within the Risk Management Toolkit enable risk analysts to effectively decompose a system and understand its risk profile. However, in addition to being equipped with a thorough and principled understanding of these methods, risk groups must also have certain characteristics to be most effective. Our experiences in partnering with numerous organizations have afforded us a unique perspective in identifying these organizational characteristics and understanding why they are so essential for effective ERM. In the section below, we enumerate and describe these characteristics as well as how they often factor into an enterprise's risk management program.

To be most effective in managing and responding to enterprise risks, organizations should have:

(1) *A workforce trained in modern methods of risk management*. The most effective risk management groups are staffed with individuals who, in addition to having relevant domain knowledge, are trained in the methods that represent the current state-of-the-practice in risk management. This includes mastery of the Risk Management Toolkit as described above, as well as understanding the appropriateness of each tool given the situation or analytical need. Moreover, the risk group should prioritize continuous improvement through training programs and knowledge transfer at trade conferences.

(2) *An adept data processing and exploitation pipeline*. The outputs of a risk analysis are only as good as the quality of its inputs. Therefore, great care should be taken to ensure that data collection systems are reliable and standardized, that data are easily accessible by risk analysts and managers, and that data are used appropriately. According to University of California - Berkeley's School of Information, the data science life cycle involves five stages: capture, process, maintain, analyze, and communicate [30]. We suggest a simplified version pertaining to ERM that includes two components: data processing and data exploitation. Data processing involves the collection, movement, and reporting of data. An organization's data processing pipeline should be strategically designed to ensure that data are exploitable for risk analysis with minimal friction.

Data exploitation involves the use of various algorithms—such as text mining and regression—to extract helpful information for the purpose of ERM. At the various points of collection (field operator data inputs at a remote site, state of health sensors, etc.), data systems should be designed to facilitate ease of use by the analysts. For example, this may also include minimizing the amount of unstructured data entry in the pipeline. The collected data should freely flow from point of collection to data stores at the operational unit, and ultimately to the enterprise risk or data analysis groups with minimal impediments from organizational or process overhead. Once at the point of analysis, data analytics and risk management products should also adhere to a standardized set of output formats to ensure consistency of interpretation. These results should finally flow back to the operational units with minimal friction in a form that is understandable to the end customers. Ultimately, a well-designed data processing and exploitation pipeline enables faster and more efficient risk analysis of systems.

(3) *A thorough codification of the Risk Management Toolkit*. The concepts that comprise the Risk Management Toolkit should be codified in a set of coherent documents that serve as the "operational Bible" for the enterprise risk management group. A set of standard operating procedures, runbooks, playbooks, and reference guides should be built and maintained, which enable risk analysts to build appropriate analytical tools to perform risk management.

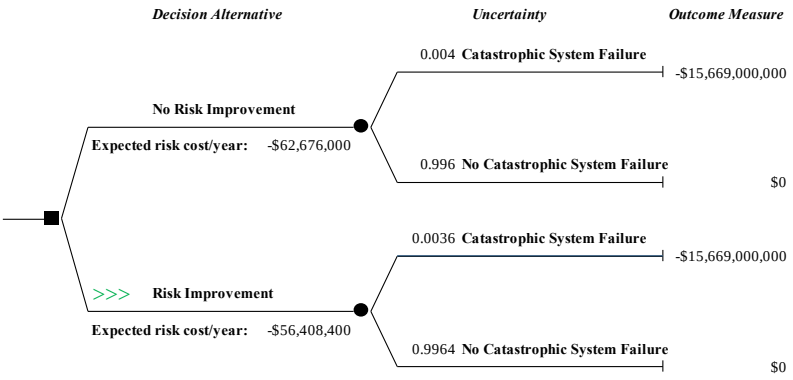
(4) *A normative decision-making framework*. As described in Section 3.1., a normative decision-making framework is required to make unbiased, rational operational decisions given the analytical results from a risk model. This not only ensures that decision makers are informed and equipped to make optimal decisions in a clear and objective manner, but also aids communication of risk management decisions to executive leadership, the board, regulators, and other stakeholders.

5. ECONOMIC JUSTIFICATION OF ENTERPRISE RISK MANAGEMENT

For organizations to mature their risk management capabilities from qualitative methods to the methods in the Risk Management Toolkit, significant investments in intellectual capital and training are required. Rarely is this transformation possible through existing internal means, principally because such transformation requires thorough knowledge of methods and practices not already in place within the organization. Therefore, most organizations require outside consultancy to facilitate this change. We claim that successful deployment of quantitative risk management methods can yield significant returns on investment. In working with executive leadership of large public utilities, we have found that, initially, the value proposition associated with new investments in risk consultancy is poorly understood. Executives often resist these investments because the economic benefits are not immediately clear. For this reason, it is useful to provide an economic analysis to demonstrate the overwhelming value associated with investments in modernizing enterprise risk management capabilities.

To illustrate the economic benefit of this effort, consider the following simplified decision model. In this example, we begin by examining an investor-owned utility in California: Southern California Edison (SCE). We utilize financial data that is publicly available at SCE's 2020 Annual Report [31] and use a narrowly scoped test case by examining only SCE's transmission infrastructure.

Figure 2. Economic analysis of risk management effort, depicted as a decision tree.



For modeling simplicity, we assume that SCE is concerned only with catastrophic failure of their electric transmission system, which would result in the total loss of service. Given the existing controls and mitigations in place, SCE's transmission assets have some degree of built-in resiliency to catastrophic events, but there exist fundamental aleatory uncertainties from both internal and external sources. Internal sources of catastrophic failure may include large scale parts failure and system-wide software failure, which may result in the crippling of the entire transmission system. External causes of system failure may include large scale flooding (such as so-called "100-year floods"), an unprecedented climate event (as evidenced by the massive freeze that struck Texas and neighboring states in February 2021, which disrupted large swaths of Texas' energy distribution services), widespread wind events, acts of terrorism, or even internal sabotage of SCE's transmission system. Given a broad encapsulation of all sources of catastrophic failure into a single failure risk event, suppose such an event will occur once every 250 years. Then the annual probability of such an event can be estimated as 1/250, or 0.004.

According to SCE's 2020 annual report, the total monetary value of SCE's transmission infrastructure is $15.669B [32]. Using this as a monetary proxy for failure consequence (though we could have used some other measure such as lost revenue), the expected risk costs per year associated with SCE's transmission infrastructure is -$62.676M. (By convention, in this analysis we denote costs with a negative sign.) One interpretation of this value is, SCE should be willing to pay approximately $63M per year to remove the intrinsic risk of catastrophic failure of its transmission system.

Now suppose that as a result of intervention, possibly in the form of expert consulting to modernize the corporation's ERM capabilities, we can assume that SCE is able to reduce 10% of the baseline catastrophic risk in the transmission system. Further, assume that such improvements in risk management require an investment of $1.5M per year for expert risk management consulting, which is a representative cost for a team of subject matter experts. Over a notional four-year period, which is a reasonable amount of time to facilitate transformational change, and given a 3% discount rate, the present value of the total risk management improvement cost is -$5.576M.

Table 1. Inputs to the decision tree.

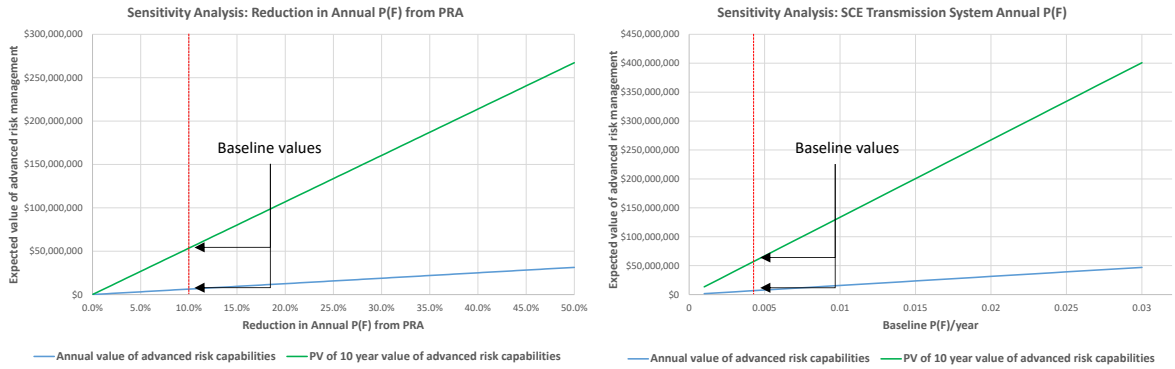
Model Input	Value	Notes
Value of transmission assets (risk cost)	-$15,669,000,000	Source: SCE Annual Report 2020, Property, Plant, and Equipment
Pre-risk management improvement *P(F)* per year	0.004	Value implies one catastrophic event every 250 years
Reduction in *P(F)* from risk improvements	10%	Estimate assumes 10% improvement over baseline
Post-risk management improvement *P(F)* per year	0.0036	Value implies one catastrophic event every 278 years
Discount rate	0.03	Representative discount rate
Annual risk consulting cost	-$1,500,000	Representative risk consulting cost to facilitate transition from legacy to modern methods of risk management
Present value of 4-year effort	-$5,575,648	Present value of risk consulting effort, assuming 4-year transition period

Model Output	Value	Notes
Annual value of advanced risk capabilities	$6,267,600	Realized reduction in risk costs per year
Present value of 10-year value of advanced risk capabilities	$53,463,899	Present value of risk reduction benefit over 10 years

Given the 10% reduction in the catastrophic failure risk of the transmission system, the annual probability of catastrophic failure is now 0.0036, which implies that a catastrophic event will now become a "once every 278-year" event. Then the revised expected risk cost per year associated with SCE's transmission infrastructure is -$56.408M, which is a reduction of expected risk costs from the baseline of -$62.676M. In other words, the annual value of risk management consultancy leading to the successful adoption and implementation of the Risk Management Toolkit is $6.268M (computed from -$56.408M - (-$62.676M)). Over a ten-year period, given a discount rate of 3%, the present value of the risk reduction benefit is $53.464M. In financial terms, over the ten-year period, SCE's return on investment (ROI) for risk management improvement costs would be over 950%. Figure 2 and Table 1 provide this economic analysis in decision tree form with accompanying inputs, respectively.

In this economic analysis, we acknowledge that key inputs, such as the annual probability of catastrophic failure of SCE's transmission system and the risk reduction improvements from the adoption of the Risk Management Toolkit, are merely point estimates. Therefore, it is appropriate to perform sensitivity analyses on these model parameters. As demonstrated by the curves of annual and present value in Figure 3, the analysis is very robust to changes in the assumed baseline annual failure probability and reduction in annual failure probability from enhanced risk management. Even if SCE's transmission system were much more resilient against catastrophic failure than initially assumed, or if adoption of the Risk Management Toolkit is not as efficacious as initially assumed, the investment in this effort still results in a highly favorable ROI. Moreover, if the risk state of SCE's transmission system is even more significant than we initially assume, then the present value of the risk reduction benefit over a 10-year period will increase dramatically. Finally, it should be noted that in this simplified economic analysis model, we do not include the risk reduction benefits of other systems, such as SCE's distribution and generation systems. It can be reasonably assumed that initial investments toward improving SCE's transmission risk management capabilities will simultaneously result in failure risk cost reductions in other systems such as distribution and generation as well. This will result in even greater overall reduction in operational risk costs, and ultimately improvements to SCE's bottom line.

Figure 3. Sensitivity analysis on baseline economic analysis with respect to (Left) baseline probability of system failure, (Right) the reduction in the baseline probability of failure.



As demonstrated herein, the value of advanced risk management capabilities is significant for operators of all energy systems, including electric, gas, renewable, and nuclear operations. Though some executives may initially resist such investments due to the perceived lack of economic benefit, this analysis reveals that the benefits are clear and overwhelming.

6. CONCLUSION

Effective ERM creates value for an organization by enabling it to pursue its mission more successfully. Furthermore, effectively managed operational risks and reduced risk costs allow for clear communication with internal and external stakeholders, as well as transparency to the public. While many of the examples throughout this article are drawn from our work with the energy sector, the improvements and innovations to current ERM practices that we describe generalize to all sectors and industries. It is important to note that the efficacy of an ERM unit is inextricably tied to the commitment of its leadership. Indeed, the technical foundations that we present throughout this article describe the first steps executive leaders should consider towards a future with fewer lives and property lost due to risk oversight. Ultimately, when enterprise risk is managed rigorously and thoughtfully, organizations are empowered to continue pursuing their missions and driving economic growth for society.

References

[1] G. Bridge, B. Özkaynak and E. Turhan, "Energy infrastructure and the fate of the nation: Introduction to special issue," *Energy Research & Social Science,* vol. 41, pp. 1-11, July 2018.

[2] Butte County District Attorney, "The Camp Fire Public Report. A Summary of the Camp Fire Investigation," June 2020.

[3] "PG&E pleads guilty to 84 counts of manslaughter in 2018 Camp Fire".

[4] Joseph, Maxwell B., et. al., "Spatiotemporal prediction of wildfire size extremes with Bayesian finite sample maxima," *Ecological Applications,* vol. 29, no. 6, p. e01898.

[5] B. W. Nocco and R. M. Stulz, "Enterprise Risk Management: Theory and Practice," *Journal of Applied Corporate Finance,* vol. 18, no. 4, p. 8–20, 2006.

[6] R. E. Hoyt and A. P. Liebenberg, "The Value of Enterprise Risk Management," *Journal of Risk and Insurance,* vol. 78, no. 4, p. 795–822, 2011.

[7] Performance Improvement Council, "Playbook: Enterprise Risk Management for the U.S. Federal Government," July 2016.

[8] C. Danner and P. Schulman, "Rethinking Risk Assessment for Public Utility Safety Regulation," *Risk Analysis,* vol. 39, no. 5, p. 1044–1059, 2019.

[9] E. Aven and T. Aven, "On the Need for Rethinking Current Practice that Highlights Goal Achievement Risk in an Enterprise Context," *Risk Analysis,* vol. 35, no. 9, p. 1706–1716, 2015.

[10] N. Komendantova, et. al., "Multi-hazard and multi-risk decision-support tools as a part of participatory risk governance: Feedback from civil protection stakeholders," *International Journal of Disaster Risk Reduction,* vol. 8, p. 50–67, June 2014.

[11] L. A. Cox, "What's Wrong with Risk Matrices?," *Risk Analysis,* vol. 28, no. 2, p. 497–512, April 2008.

[12] "Lessons learned from the real world application of the bowtie method".*Risktec.*

[13] State of California Public Utilities Commission, "Proposed Decision of Commissioner Rechtschaffen to Parties of Record in Application 15-05-002 ET AL," 2018.

[14] State of California Public Utilities Commission, "Proposed Decision of Commissioner Rechtschaffen to Parties of Record in Application 15-05-002 ET AL," 2018.

[15] "Pacific Gas and Electric Company 2020 Risk Assessment and Mitigation Phase Report," 2020.

[16] "This Old Metal Hook Could Determine Whether PG&E Committed a Crime - WSJ".

[17] G. Montibeller and D. v. Winterfeldt, "Cognitive and Motivational Biases in Decision and Risk Analysis," *Risk Analysis,* vol. 35, no. 7, p. 1230–1251, 2015.

[18] A. E. Abbas, "Constructing Multiattribute Utility Functions for Decision Analysis," in *INFORMS*, 2010.

[19] A. J.Brito, A. T. Almeida and C. M. Mota, "A multicriteria model for risk sorting of natural gas pipelines based on ELECTRE TRI integrating Utility Theory," *European Journal of Operational Research,* vol. 200, no. 3, p. 812–821, 2010.

[20] E. J. Cha and B. R. Ellingwood, "The role of risk aversion in nuclear plant safety decisions," *Structural Safety,* vol. 44, p. 28–36, September 2013.

[21] C. A. Cornell, "Engineering Seismic Risk analysis," *Bulletin of the Seismological Society of America,* vol. 58, no. 5, p. 1583–1606, October 1968.

[22] G. Massimo, L. Mara and M. Federica, "Risk Analysis in Handling and Storage of Petroleum Products," *American Journal of Applied Sciences,* vol. 10, no. 9, p. 965–978, September 2013.

[23] L. Guerra, T. Murino and E. Romano, "Airport System Analysis: A Probabilistic Risk Assessment Model," *International Journal of Systems Applications, Engineering, & Development,* vol. 2, no. 2, 2008.

[24] T. Cho and T. S. Kim, "Probabilistic Risk Assessment for the Construction Phases of a Bridge Construction Based on Finite Element Analysis," *Finite Elements in Analysis and Design,* vol. 44, no. 6, p. 383–400, April 2008.

[25] J. Wreathall and C. Nemeth, "Assessing Risk: The Role of Probabilistic Risk Assessment (PRA) in Patient Safety Improvement," *Quality and Safety in Health Care,* vol. 13, no. 3, p. 206–212, June 2004.

[26] "Number of homes destroyed in San Bruno explosion now at 38 – The Mercury News".

[27] California Public Utilities Commission, "Consumer Protection & Safety Division September 9, 2010 PG&E Pipeline Rupture in San Bruno, California," 2012.

[28] M. Farshad, "Fatigue, Corrosion, and Wear," *Plastic Pipe Systems, Oxford: Elsevier Science,* p. 153–165, 2006.

[29] R. Kim, "Stochastic Inventory Control Modeling for Satellite Constellations," *Journal of Spacecraft and Rockets*, vol. 57, no. 3, p. 612–620.

[30] "What is Data Science? | The Data Science Career Path," *UCB-UMT.*

[31] Edison International, "Edison International and Southern California Edison 2020 Annual Report".