The Mission Dependency Index: Fallacies and Misuses

Edouard Kujawski
Department of Systems Engineering
Naval Postgraduate School
Monterey, CA 93943
Email: ekujawsk@nps.edu
Telephone: (831) 656 3324

Gregory Miller
Department of Systems Engineering
Naval Postgraduate School
Monterey, CA 93943

Abstract. The U.S. infrastructure is extensive and faces performance, physical deterioration, natural disaster, terrorism, and social challenges. The problem is further compounded by the fact that funds are limited. Decision-makers need to prioritize their assets on the basis of risk and allocate budgets accordingly. The response to this situation has been the quest for a simple equation that quantifies risk in terms of ordinal numbers. Unfortunately, most proposed risk indices are seriously flawed and likely to lead to bad decisions. This paper first focuses on the Mission Dependency Index (MDI) as an example of an over-simplified model that has gained wide acceptance for ranking facility risk. It then proposes the Operational Risk Failure Modes and Effects Analysis (ORFMEA) as a rational method for analyzing potential threats to facilities and link to missions. The ORFMEA enhances the standard Operational Risk Management (ORM) assessment by incorporating vulnerability and facility/mission time criticality.

Introduction

The U.S. infrastructure is extensive and faces technology, physical deterioration, natural disaster, terrorism, financial, and social challenges. Many of these systems are vulnerable to disruptive events such as terrorist attacks, natural disasters, and technological failures (or accidents). These problems are not new. Even prior to 9/11, the Clinton administration developed a policy on critical infrastructure protection (PDD-63) that called for a national effort to assure the security of the increasingly vulnerable and interconnected infrastructures. The infrastructure management problem is further compounded by the fact that (1) funds for sustainment and renovation are limited, (2) many of the analyses are inadequate or flawed, and (3) decisions for maintenance, improvements, or replacements are often driven by hidden agendas.

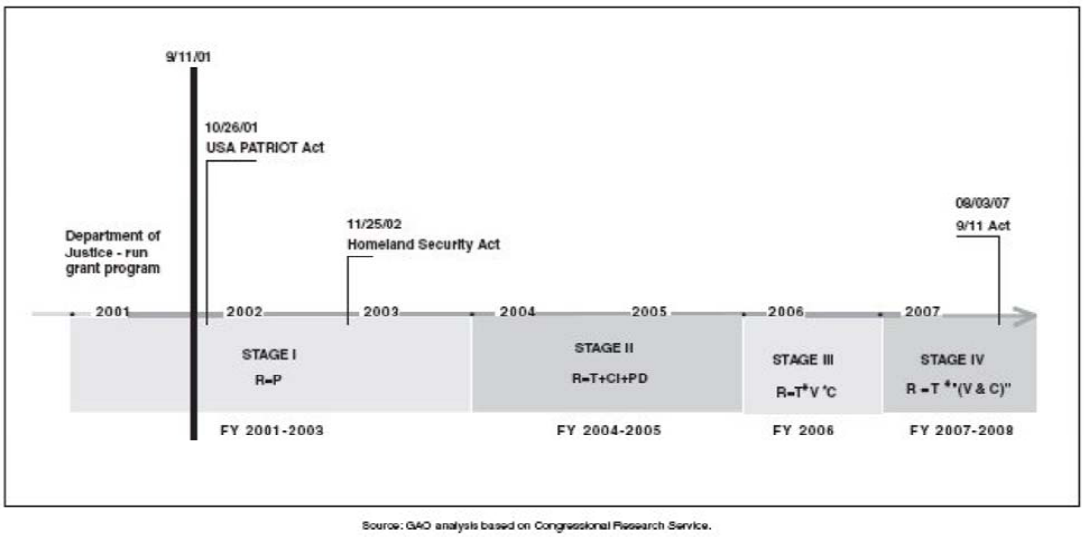
In 2005 the G. W. Bush administration released DoDD 3020.40, the Defense Critical Infrastructure Program (DCIP) directive (U.S. Department of Defense 2005). It includes the following two policy statements that explicitly address risk assessment and management:

> *"4.2. Vulnerabilities found in Defense Critical Infrastructure shall be remediated and/or mitigated based on risk management decisions made by responsible authorities.*

4.3. The identification, prioritization, assessment, and assurance of Defense Critical Infrastructure shall be managed as a comprehensive program that includes the development of adaptive plans and procedures to mitigate risk, restore capability in the event of loss or degradation, support incident management, and protect Defense Critical Infrastructure related sensitive information."

Risk management is not limited to critical infrastructures. An increasing number of facility managers and decision-makers are applying it to allocate their limited resources to the areas most at risk. On the surface this appears to be an excellent idea; but the devil is in the details. Risk is an intuitively familiar concept; but it is complex and difficult to assess. There is overwhelming evidence that many rational people act more on the potential magnitude than the probability of an undesirable outcomes (Kahneman and Tversky 1979; Tversky and Kahneman 1992). In theory, the results of a quantitative risk analysis are best quantified and reported using risk profiles. Risk profiles provide information about extreme outcomes, which is important for sound decision-making. Unfortunately, the typical analyst is challenged with communicating the results to the typical decision-maker who may possess limited probabilistic thinking skills to comprehend risk curves. The response to this situation has been the quest for a silver bullet; i.e. a simple equation that quantifies risk in terms of a single number that ranges from 1 to 100 or 1 to 4. Even the distinguished 9/11 Commission (2001, 396) asked: *"Can useful criteria to measure risk and vulnerability be developed that assess all the many variables?"* But this was intended mainly as a rhetorical question that the 9/11 Commission immediately answered with the following insightful observations: *"The allocation of funds should be based on the assessment of threats and vulnerabilities....The benchmarks will be imperfect and subjective; they will continue to evolve. But hard choices must be made. Those who allocate money on a different basis should then defend their view of the national interest."*

Over the past several years, numerous simple quantitative risk models have been proposed to aid decision-making. To the best of the authors' knowledge, a silver bullet has not yet been developed. The Department of Homeland Security (DHS) is still struggling to develop a satisfactory formula to allocate funds that recipient states and urban areas think are equitable. Figure 1 depicts the evolution of the Department of Homeland Security's risk-based formula. It should be noted that DHS documentation very clearly defines the key terms Threat, Vulnerability and Consequences. While the ultimate quantification of risk itself is not entirely consistent with the traditional theory and practice of risk management, DHS's method represents a logical and workable extension. Further, efforts are underway to mitigate the usual flaws associated with simplified models. The problem is not limited to DHS. Numerous agencies have inadequately spent and are still inadequately spending significant funds. Anderson et al. (2008) state: *"methodologies have been developed to comply with DCIP initiatives (e.g., DoD, 2003, 2004, 2006)…We maintain that some of these methodologies are highly subjective and lack appropriate intermediate analysis."*



Source: GAO analysis based on Congressional Research Service.

Definitions for the formulas above:
R = P represents Risk = Population;
R = T+CI+PD represents Risk = Threat plus Critical Infrastructure plus Population Density;
R = T*V*C represents Risk = Threat times Vulnerability times Consequences;
R = T* "(V&C)" represents DHS's presentation of the risk calculation formula used in their risk analysis model for 2007 and 2008: Risk = Threat times the combination of Vulnerability and Consequences. However, in the 2007 and 2008 risk analysis models, the combination of vulnerability and consequence is still calculated as the product of V times C, or R = T*V*C.

Figure 1. Evolution of DHS's risk-based formula (U.S. GAO 2008).

The risk of over- simplified models is that they tend to provide distorted risk pictures and thereby could mislead decision-makers. This idea is not new, and numerous researchers have cautioned against over-reliance on quantitative decision tools (Brown 2003; Saari 1999). To further aggravate the situation, facility managers and decision-makers who need to prioritize their assets on the basis of risk and allocate budgets in accordance with benefits also face pressure from self-interest groups.

In this paper we focus on the MDI as an example of an over-simplified model that has gained wide acceptance for categorizing facilities (Naval Facilities Engineering Command 2008). The MDI is now used by the Naval Facilities Engineering Command (NAVFAC), the United States Coast Guard (USCG) Office of Civil Engineering and the National Aeronautical and Space Administration (NASA) as a risk-based metric that links facilities to mission (Antelman et al 2008). The US General Services Administration recognizes it as a "Best Practice." The Federal Facilities Council in its 2005 report on key performance indicators for federal facilities writes (Cable and Davis 2005, 29): *"A promising process indicator for prioritizing projects and funding to support an organization's overall mission is the Mission Dependency Index (MDI)."*

The Mission Dependency Index Methodology

The MDI was first defined at the Naval Facilities Engineering Service Center in the spring of 2000 and has from early inception been co-developed with the US Coast Guard's Office of Civil Engineering. While the authors understand the desire to support

sustainment and renovation funding decisions based on a clear and quantifiable connection between facility risk and mission execution, the method does little to mitigate the flaws of any simplifed risk assessment method. It represents a significant deviation from classical operational risk management (ORM) methods. The MDI, it is purported, quantifies the importance or criticality of a facility's mission in terms of an algebraic expression that depends on two facility-intrinsic measures (interruptabilty, relocateability or replaceability) rather than probability and severity:

$$MDI = 26.54 \times \left[MD_w + 0.125 \times \frac{1}{n} \sum_{i=1}^{n} MD_{bi} + 0.1 \times \ln(n) \right] - 25.54 \qquad (1)$$

- MD_w is the mission intradependency (the *w* subscript indicates "within missions"). It accounts for the importance of the missions that are controlled within the facility. It is determined by asking mission operators the following two questions (Antelman et al. 2008):

Question #1 (Q1) addresses the interruptability of the facility functions as follows:

> *"How long could the functions supported by your facility be stopped without adverse impact to the mission?"*

Question #2 (Q2) addresses the relocateability or replaceability of the functions as follows:

> *"If the facility were no longer functional, could you continue performing your mission by using another facility or by setting up temporary facilities?"*

The response to each question is one value on a four-point Likert scale. The definitions of the values are provided. For example, "Brief" is defined as "minutes or hours, not to exceed 24 hours" (Antelman et al 2008). Based on the answers, the numerical score for MD_w is obtained using the matrix in Figure 2.

- MD_{bi} is the mission interdependency for organizational subcomponent *i* (the *b* subscript indicates "between missions or services"). It accounts for the organizational subcomponent interdependencies. It is determined similarly to MD_w where the two questions now score the impact of services or missions provided by other organizational subcomponents. Note that MDI depends on the arithmetic mean of the applicable externally-provided services.

- *n* is the number of mission interdependencies.

The MDI scores are divided into 5 categories that are color-coded and assigned verbal terms suggestive of the mission importance as depicted in Figure 3. The MDI Eq. (1) along with the MD_w and MD_b matrices in Figure 2 and the MDI score vector in Figure 3, or variations of it, is in use by the Coast Guard, Navy, NASA, and the Army Corps of Engineers. For a typical facility, an hour-long interview with the operational manager suffices to determine the facility intrinsic-measures.

Q2: Relocateability	Q1: Interruptability of Function			
	Immediate (24/7)	Briefly ≤ 24 hrs	Short 1 to 7 days	Prolonged > 7 days
Impossible	4.0	3.6	3.2	2.8
X Difficult	3.4	3.0	2.6	2.2
Difficult	2.8	2.4	2.0	1.6
Possible	2.2	1.8	1.4	1.0

Impossible: There are no viable commercial alternatives – only this site/command can provide these services.
Extremely Difficult: There are viable commercial alternatives, but no readily available contract mechanism in place to replace the services.
Difficult: Services exist and are available, but the form of delivery is ill defined or will require a measurable and unbudgeted level of effort to obtain (money/man-hours), but mission readiness capabilities would not be compromised in the process.
Possible: Services exist, are available, and are well defined.

Figure 2. The MDI intradependency matrix with the more recent values of Antelman et al. (2008). The criticality associated with the MDI is depicted in Figure 3. The MDI interdependency matrix is identical with "Replaceability" substituted for "Relocateability".

MDI score	Verbal code	Color code
100 - 85	Critical	Red
84 - 70	Significant	Orange
69 - 55	Relevant	Yellow
54 - 40	Moderate	Green
39 - 1	Low	Blue

Figure 3. The MDI numerical scores with associated verbal and color codes. The scores and codes are indicative of the criticality of the facility.

Some MDI Fallacies

We critically examine several claims made by the MDI developers (Antelman et al. 2008).

Fallacy 1. *"The MDI uses Operational Risk Management techniques of probability and severity and applies them to facilities in terms of interruptability, relocatability and replaceability…Responses are recorded and intra-dependency scores are determined using the Risk Assessment Matrix based on OPNAVINST 3500.39B, Operational Risk Management (ORM)."*

The above statement is a misrepresentation of the foundation of the MDI as well as a misinterpretation of the ORM approach. For ease of comparison, we present the OPNAVINST 3500.39B (Department of the Navy 2004) risk assessment matrix in Figure 4. The risk assessment matrix expresses risk qualitatively in terms of hazard severity and mishap probability. The Arabic numbers are referred to as Risk Assessment Code (RAC) and define an ordinal scale. The use of letter-categories for severity and Roman number-categories was originally intended to prevent analysts from multiplying them. But this obstacle was no match for some analysts' drive for numbers.

OPNAVINST 3500.39B provides quantitative guidelines for the probability and severity categories to provide some degree of consistency for the subjective nature of the risk assessment. These are not depicted in Figure 4 because individual organizations need to substitute their own definitions and/or use other measures of damage and probability appropriate to their specific applications. Another critical point is that arithmetic operations such as addition and multiplication are not permitted for an ordinal scale. The MDI, unlike the ORM matrix, performs these operations on the MD_w and MD_b scores. More importantly, the MDI method makes no attempt to quantify probability and includes no discussion of mishap likelihood. This is the most serious deviation from the ORM instruction because it clearly states: *"Although different matrices may be used for various applications, any risk assessment tool should include the elements of hazard severity and mishap probability."* Several other well-known risk analysis guides state that risk analysis includes an assessment of a mishap's likelihood as well as consequences (National Infrastructure Protection Center 2002; National Infrastructure Advisory Council 2005).

		PROBABILITY			
		A	B	C	D
SEVERITY	I	1	1	2	3
	II	1	2	3	4
	III	2	3	4	5
	IV	3	4	5	5

RAC Definitions:
1 - Critical risk
2 - Serious risk
3 - Moderate risk
4 - Minor risk
5 - Negligible risk

Figure 4. The OPNAVINST 3500.39B risk assessment matrix.

Fallacy 2. *"The MDI's true power is that it is very straightforward and eloquent in its simplicity. It is risk-based and due to the structured interview process is robust enough to singularly accommodate individual decision-maker's risk-tolerances,…"*

In FY06, the Department of Energy (DoE) performed its initial MDI and concluded that there are inconsistencies in the interpretation and application of the standard definitions. In 2007, the DoE Director of Office Engineering and Construction Management (Bosco 2007) directed his staff to "establish a crosscutting team to update the MDI definitions and/or establish common guidelines for their application."

It is important to note that the MDI questions and responses do not adequately

address the time dependency of corrective actions such as design changes and work-arounds. Question # 1 (Q1) classifies the time criticality of the functions supported by the facility into four categories (Figure 2). However, Question # 2 (Q2) and the listed responses in Figure 2 seem to treat the complexity of setting up a work-around independently of the function-time criticality. As an example, consider an "immediate 24/7" function such as a life-support system in the critical care unit of a hospital. None of the four Q2 options, including "possible", are appropriate since even "possible" would result in a temporary loss of function and therefore loss of life. Having a life-support system "readily available" is not an acceptable option. The only acceptable option is redundancy with automatic fail-over. While this example may be extreme, it is representative of the challenges of adequately supporting "immediate 24/7" functions. At a minimum, Q2 should be conditional given Q1.

Fallacy 3. "*MDI can be used to prioritize funding for projects having the most positive impact."*

A few simple examples are sufficient to see that this is a fallacy. Consider the following two cases:

Case 1. A facility element like a remote air-traffic control center with interruptability and relocateability characterized as "immediate 24/7" and "difficult", respectively. The MD_w score is 2.8.

Case 2. A facility element like a steam plant on a military base in a non-combat zone. Its interruptability and relocateability are realistically characterized as "briefly $\leq$ 24 hrs" and "impossible", respectively. The MD_w score is 3.6.

To mean anything, the MD_w and MD_b matrices should be based on the workaround time (T_w) versus the function interruptability time (T_f), as addressed under Fallacy 2. This type of information is not adequately reflected in the MD_w and MD_b scores. Few rational individuals would argue that the loss of the air-traffic control center poses a lower operational risk than the loss of a steam plant on a military base in a non-combat zone, because it is easier to relocate its function. Allocating the limited funds to the Case 2 facility because it has a MD_w of 3.6 while the Case 1 facility has a MD_w of 2.8 represents a bad decision caused by the MDI process.

Fallacy 4. *"By linking facilities to mission, MDI scores simply communicate a critical and heretofore missing detail in infrastructure related decision-making."*

This is a fallacy because the MDI scores are obtained from a flawed equation. The questions used to obtain the MD values link facilities loss to mission impact, but Eq. (1) does not realistically describe the relationship and breaks down for credible facilities.

- Eq. (1) is not defined for n = 0.

This is a realistic case since not all facilities need support missions or services from external organizations.

- Eq. (2) is not valid for facilities that only provide support functions; i.e. nothing precludes facilities with $MD_w = 0$.

When $MD_w = 0$, Eq. (1) predicts MDI < 0. For example, if n = 1 and $MD_b = 4$, Eq. (1) results in MDI = -12.27.

- Eq. (1) does not adequately account for the interdependencies because the average over several supporting missions or services does not adequately quantify risk or

criticality.

Consider the following two cases:

Case 1. $MD_w = 4.0$, $n = 1$, $MD_b = 4$. Eq. (1) results in MDI = 93.89

Case 2. This case is identical to Case 1 with the exception that the facility now includes 9 additional interdependencies with each value $MD_{bi} = 1$. Eq. (1) results in MDI = 91.0.

Most rational individuals will agree that the Case 2 facility, which differs from the Case 1 facility by including nine additional interdependencies, is at a greater risk simply based on its more complicated (and hence more vulnerable) supporting infrastructure and should have the larger MDI. Reliance on Eq. (1) may lead to bad prioritizations.

Fallacy 5. *"The MDI equation and weighted coefficients are the result of three years of extensive field-testing."*

There are several scientific challenges to the validity of this statement. The first challenge is that the scores are subjective and based on questions and responses that are ambiguous (Fallacy 2). The second challenge is that Eq. (1) does not provide a realistic model for linking facilities to missions (Fallacy 4). The third challenge is that the developers did most of the testing. The problem of relying on limited information and judging results based on aggressive advocacy rather than using the scientific method is not new. Park (2000, vii) writes: "*As I sought to make the case for science, however, I kept bumping up against ideas and claims that are totally, indisputably, extravagantly, wrong, but which nevertheless attract a large following of passionate and sometimes powerful proponents*." The method for validation via field-testing is not described. Any analysis involving validating fitted polynomial curves of quantitative data requires, at a minimum, the number of samples collected, the raw data matrix, equations of the fitted models along with plotted curves and plotted raw data, quality of the fit of the curves and substantive meaning of the estimated models (Tufte 2006, 150). As this information is not presented, it is difficult to subject it to rational scrutiny to determine its support for the result (Paul et al 2006).

Failure Mode, Effects and Criticality Analysis (FMECA)

Background. The FMECA is a widely used and proven method to systematically identify potential failures, determine their effects, identify corrective or mitigation actions, and assess their criticality, qualitatively or quantitatively. It was introduced in the 1960's on the Apollo program as a design tool for increased system and component reliability. The U.S. Navy published the first widely-applicable version in Mil-Std-1629 in 1974. The FMECA approach can readily be tailored to different applications (Mil-Std-1629A, Appendix A). The FMECA is now widely accepted as a best practice for improving a wide variety of applications including manufacturing processes, services, and project risk management (Carbone and Tippett 2004).

A Failure Mode and Effects Analysis (FMEA) may be performed at the hardware or functional levels. It can also be organized around scenarios rather than failure modes (Kmenta and Ishii 2000). The FMEA, unlike the FMECA, typically employs a qualitative approach. Each failure mode is assigned to one of the following severity classification categories: catastrophic, critical, marginal, or minor.

Mil-Std-1629A also specifies a Criticality Analysis (CA), whose purpose is to rank each potential failure mode identified in the FMEA according to the combined influence

of severity classification and its probability of occurrence. The CA generates the criticality number C_r as a measure to proritize corrective actions that may be taken to eliminate or control the high-risk items. It represents the number of system failures of a particular severity classification expected due to the item's failure modes. It is rarely calculated because the required information such as (i) the failure mode ratio is not available in reliability databases including Mil-Hdbk-217, and (ii) a credible conditional probability of mission loss would require a detailed probabilitic risk analysis. (For additional details, the interested reader should consult Mil-Std-1629A.)

The Risk Priority Number (RPN). Given the complexity and lack of data necessary to calculate Cr, many FMECAs now unfortunately assess risk using the RPN (Creveling et al. 2003; Blanchard and Fabrycky 2006),

$$\text{RPN} = \text{Occurrence} \times \text{Severity} \times \text{Detection Probability}. \qquad (2)$$

Each term in Eq. (2) is typically rated using ordinal scales with the higher number representing the higher risk contributor. There is no standard rating scale. The rating scales usually range from 1 to 10 or from 1 to 5. To further confound risk comparisons, each factor may be defined on a different scale (Ben-Daya and Raouf 1996). The RPN, like the MDI, is deceptively attractive and mileading. Gilchrest (1993) states: *"Though the method itself is in great use, the calculation of the RPN lacks a proper model as a base and is thus internally inconsistent and potentially misleading."* Figure 5 depicts a sample RPN application for a process FMEA.

(PROCESS FMEA)

Item MM-2X | Process Responsibility Goodson | FMEA Number MM-2000
Model Year(s)/Program(s) 2001/N/A | Key Date 4/24/2001 | Prepared By R. Yates/867-5309
Core Team Sam and Janet Eveling | FMEA Date (Orig.) 2/2/1999 (Rev.) 03/03/2001

Process Function / Requirements	Potential Failure Mode	Potential Effect(s) of Failure	Sev	Class	Potential Cause(s)/ Mechanism(s) of Failure	Occ	Current Process Controls - Prevention - Detection	Det	RPN	Recommended Action(s)	Resp. & Target Compl. Date	Action Results: Actions Taken	Sev	Occ	Det	RPN
010 - Wind wire around index finger																
001 - Coil diameter	Diameter too large	- Coil hits battery during operation - Rotor is short because too much material is used in coils	8	0	Wire wound loosely	3	>Char Control 1: Measure with gage.	4	96	None		None				
	Diameter too small	- Weak motor - Difficult removal from finger	6		Finger too small	4		3	72	None		None				
	Diameter too large	- Coil hits battery during operation - Rotor is short because too much material is	8		Finger too large	5		3	120	None		None				

Figure 5. Illustrative application of the Risk Prioritization Number (RPN). Note that in this FMEA, Occurrence, Severity, and Detection appear to be rated on a 1 to 10 scale; to be sure one needs to read the applicable report. No meaning of quantitative risk should be assigned to the RPNs; i.e. it is not clear what risk classification to assign to RPNs of 120 vs. 96 vs. 71.

Multipying ordinal numbers is not mathematically allowed. The result is mathematically as well as logically meaningless. It is therefore alarming that the RPN, more than fifteen years after the flaw was identified, still forms the basis for many important decisions. The RPN and the MDI are not the rare flawed decision aids. Many analysts and decision-makers tend to be easily enticed by deceitfully simple quantitative methods. Given this environment, there are many examples of irrational decision-making methods. Unfortunately, some of these are practiced by poorly trained systems

engineeers (Clausing and Katsikpopoulos 2008).

The ORFMEA

Realistic models of risk are essential to efficient and robust ORM. This is a complex and difficult problem that includes the assessment of (i) threats such as system failures, natural hazards and terrorist attacks, and their likelihood; (ii) the vulnerability of systems and infrastructures; (iii) the resilience of systems and infrastructures; and (iv) the consequences. We propose to incorporate these risk criteria by adding qualitative vulnerability and resilience assessments to the five-step ORM process of OPNAVINST 3500.39B. The FMEA, with its systematic framework and reliance on people with direct knowledge of the facilities and links to missions, is well suited to this task. The additional fields in a spreadsheet format are shown in Figure 6. More general and convenient formats can readily be prepared using database software. The score in the Risk column is assessed in terms of the two classical risk criteria – Frequency and Consequences – and the three additional criteria – Vulnerability, Interruptability, and Reloceatability – as described below.

Operational Risk Management
Failure Mode and Effects Analysis

Facility D .
Mission X .
Prepared by J. Doe

Item/Element	Function	Threat	Frequency	Consequence	Vulnerability	Interruptability	Relocatability	Risk	Remarks
		W	P	H	H	B	B	H	

Figure 6. Sample operational risk management failure modes and effects analysis format.

Assessing Key Risk Attributes

Before continuing, some discussion of the attributes of a good risk-based decision support tool is warranted. Decision support tools bring discipline to the sometimes chaotic process of selecting alternatives in a manner reflective of decision-maker values, particularly those associated with cost and benefit associated with the alternatives. A general methodology for integrating risk management and resource allocation has been developed: 1) Identify critical assets, 2) Identify and assess potential threats, 3) Identify and assess vulnerabilities, 4) Identify and assess consequences, 5) Assess baseline risk, 6) Identify risk management alternatives and 7) Select the most cost-effective alternative. Here, steps 2) and 3) are performed in parallel, with the results informing steps 4) and 6) (Parnell et al 2005). Threat assessment must include estimates of probability of occurrence. The assessment of consequences should be couched in terms of mission impact. That is, the connection between mission function and the facility under consideration should be made explicit. Of course, “most cost-effective” is defined in terms of the decision-makers values. Reliance on performing mathematical functions on non-rational numbers should be avoided. We propose to assess the key risk attributes of

the proposed ORFMEA using the rational approach presented below.

Frequency-Vulnerability. Frequency of a threat is qualitatively assessed in accordance with OPNAVINST 3500.39B sub-categories A, B, C and D. However, the probability of a terrorist attack is not independent of vulnerability. Vulnerability is defined as both (i) a characteristic of an asset's design, implementation, or operation that affects its ability to withstand threats, and (ii) the probability that a particular attack will succeed (US Government Accountability Office 2008, 20). One cannot reliably predict the absolute frequency of terrorist threats. However, it is reasonable to assume that the relative frequencies are proportional to vulnerability (Parnell et al 2005; Kujawski and Miller 2007).

Vulnerability is recognized as a weakness in the DHS' risk-based methodology. The US Government Accountability Office's report on homeland security (2008, 25) concludes: "*Vulnerability is a crucial component of risk assessment, and our work shows that DHS needs to measure vulnerability as part of its risk analysis model to capture variations in vulnerability across states and urban areas.*" Consistent with the proposed qualitative approach, vulnerability is assessed as High, Medium, Low against some specified criteria. Figure 7 depicts a reasonable frequency-vulnerability risk factor matrix for determining the criticality of the aggregate factor (the frequency category of "unlikely" has been removed for clarity in this example).

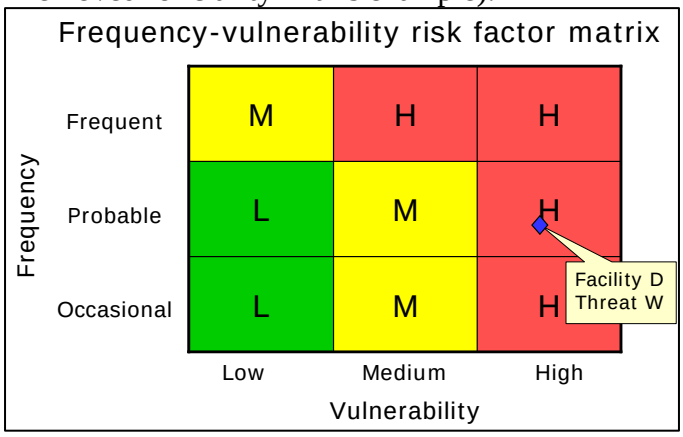


Figure 7. Sample frequency-vulnerability risk factor matrix.

Facility-mission time criticality. As discussed for Fallacy 3, the relocateability time versus the function interruptability is of critical importance to risk. A rational treatment of this relationship may be as follows:

If $T_w > T_r$, then the facility/mission time criticality is high
If $T_w \sim T_r$, then the facility/mission time criticality is medium
If $T_w < T_r$, then the facility/mission time criticality is low,

where T_w is the function interruptability time and T_r is the relocateability (replaceability) time. These relationships can be captured in a facility-mission criticality risk factor matrix as shown in Figure 8.

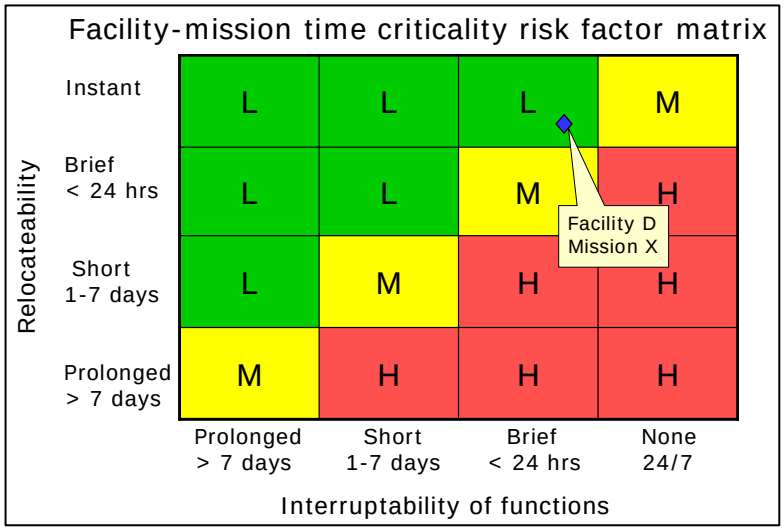


Figure 8. Sample facility-mission time criticality risk factor matrix.

The facility-mission time criticality is a resilience factor, which has a significant impact on consequences. A score of Low means that there is adequate time to recover before the mission is impacted. In contrast, a score of High means that there is inadequate time to mitigate the loss of function before the mission is impacted. The ORFMEA determines a mitigated-consequences risk factor matrix as depicted in Figure 9. The "Consequences" entering argument represents the mission impact with no relocation or replacement of the original element.

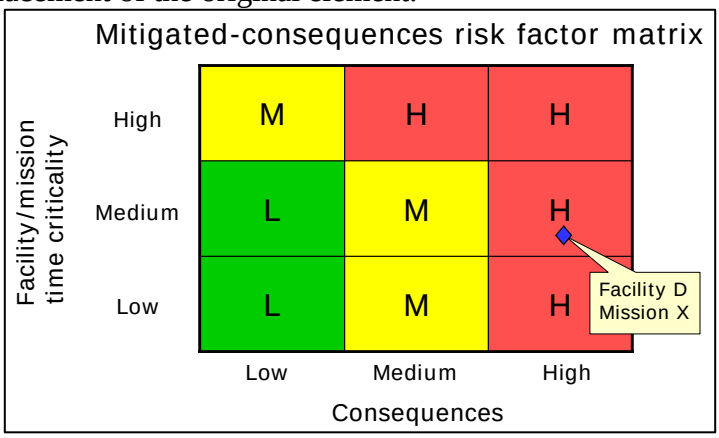


Figure 9. Sample mitigated-consequences risk factor matrix.

The ORFMEA risk assessment matrix. The final step in the ORFMEA process is to aggregate the frequency-vulnerability risk factor matrix (Figure 7) and the mitigated-consequence risk factor matrices (Figure 9) to yield an effective risk assessment matrix as depicted in Figure 10. Thus, ORM direction to include an assessment of mishap probability as well as severity is met. The risk for the scenario (Facility D, Threat W, Mission X) is obtained by first computing the frequency-vulnerability factor and the mitigated-consequences factors using the risk-factor matrices in Figures 7 and 9,

respectively.

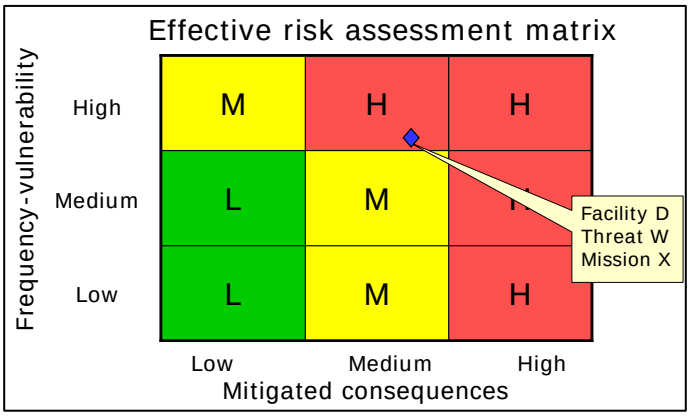


Figure 10. A sample ORFMEA risk assessment matrix.

Concluding Remarks

The need to support decisions on sustainment and renovation funding by connecting facilities to mission accomplishment is a noble goal. However, the currently favored method is fraught with peril. Multiplication and addition of ordinal numbers is mathematically as well as logically meaningless. The paper presents several simple but realistic examples where the MDI leads to irrational results. The MDI is not the rare example of a flawed decision aid. The paper also briefly discusses the RPN as an example of a tool that still forms the basis for many important safety decisions more than fifteen years after its flaws were identified. Many analysts and decision-makers tend to be easily enticed by deceptively simple quantitative methods. The MDI and RPN may make some individuals' eyes light up. Unfortunately, they also carry unintended consequences. Unknowing decision-makers may rely on these flawed aids and misallocate funds. There are numerous other examples of irrational decision-making methods. Unfortunately, some of these are practiced by poorly trained systems engineers (Clausing and Katsikpopoulos 2008). It is important for good systems engineers to be wary of methods that claim to quantify complex concepts like risk using single numbers.

As an alternative, the paper then proposes a modified FMEA/FMECA method, referred to as ORFMEA, as a rational method for analyzing potential threats to facilities and links to missions consistent with ORM. It is also consistent with the model presented by the National Infrastructure Protection Center (2002) and the United Kingdom (HM 2006). The ORFMEA explicitly incorporates vulnerability and resilience into risk. We acknowledge that the effort is more challenging than with MDI. However, given the importance of properly assessing risk and taking corrective actions, there is little excuse for relying solely on MDI. The next step is to conduct a pilot project to refine and demonstrate the applicability and validity of the ORFMEA.

References

Anderson, W. C., Barker, K., and Haimes, Y. Y. 2008. Assessing and prioritizing critical assets for the United States army with a modified RFRM methodology. *Journal of Homeland Security and Emergency Management* 5 (1): Article 5.

Antelman A., Dempsey, J.J. and Brodt, B. 2008. Mission dependency index - a metric for determining infrastructure criticality. International Facility Management Association Facility Management Workshop 2008. Washington, DC.

Ben-Daya, M. and Raouf, A. 1996. A revised failure mode and effects analysis model. *International Journal of Quality and Reliability Management* 13 (1): 43–47.

Blanchard, B. S. and Fabrycky, W. J. 2006. *Systems engineering and analysis, 4th ed*. Upper Saddle River, NJ: Prentice Hall.

Brown, R. 2003. How "decision aid" can mislead deciders due to conflicts of interest. Decision Analysis Working Paper Abstract Archive WP030012. `http://fisher.osu.edu/~butler_267/DAPapers/WP030012.html`. Accessed November 14, 2008.

Bosco, P. 2007. Memorandum dated March 12 2007. Subject: Application of the mission dependency index. Washington, DC: Department of Energy.

Cable, J. H. and Davis, J. S. 2005. Key performance indicators for federal facilities portfolios. Federal Facilities Council Technical Report #147. Washington, D.C.: The National Academies Press.

Carbone, T. A. and Tippett, D. D. 2004. Project risk management using project risk FMEA. *Engineering Management Journal* 16 (4): 28-35.

Clausing, D. P. and Katsikopoulos, K. V. 2008. Rationality in systems engineering: beyond calculation or political action. *Systems Engineering* 11 (4): 309-328.

The Clinton's Administration's Policy on Critical Infrastructure Protection: Presidential Decision Directive 63, White Paper, May 22, 1998 (PDD-63).

Creveling, C. M., Slutsky, J. L., and Antis, Jr. D. 2003. *Design for six sigma in technology and product development*. Upper Saddle River, NJ: Prentice Hall PTR.

Gilchrist, W. 1993. Modeling failure modes and effects analysis. *International Journal of Quality and Reliability Management* 10 (5): 16–23.

HM Government, "Countering International Terrorism: The United Kingdom's Strategy." http://www.ukresilience.gov.uk/media/ukresilience/assets/countering.pdf. Accessed February 28, 2009.

Kahneman, D. and Tversky, A.1979. Prospect theory: an analysis of decisions under risk. *Econometrica* 47: 13-327.

Kmenta, S. and Ishii, K. 2000. Scenario-based FMEA: a life cycle cost perspective. In Proceedings of the 2000 ASME Design Engineering Technical Conference (Baltimore, MD).

———. 2004. Scenario-based failures modes and effects analysis using expected cost. *Journal of Mechanical Design* 126: 1027–1035.

Kujawski, E. and Miller, G. A. 2007. Quantitative risk-based analysis for military counterterrorism systems. *Systems Engineering* 10(4): 273-289.

National Commission on Terrorist Attacks Upon the United States. 2004. *The 9/11*

commission report. New York, NY: W. W. Norton & Company.

National Infrastructure Advisory Council. 2005. Risk management approaches to protection. `http://www.dhs.gov/xlibrary/assets/niac/NIAC_RMWG_-_2-13-06v9_FINAL.pdf.` Accessed November 18, 2008.

National Infrastructure Protection Center. 2002. Risk management: an essential guide to protecting critical assets. `http://www.au.af.mil/au/awc/awcgate/nipc/risk_management.pdf.` Accessed November 18, 2008.

Naval Facilities Engineering Command. 2008. `https://portal.navfac.navy.mil/portal/page/portal/navfac/navfac_ww_pp/navfac_nfesc_pp/mdi.` Accessed November 13, 2008.

Park, R. L. 2000. *Voodoo science: the road from foolishness to fraud*. New York, NY: Oxford University Press.

Parnell, G. S., Dillon-Merrill, R. L., and Bresnick, T. A. 2005. "Integrating Risk Management with Homeland Security and Antiterrorism Resource Allocation Decision-Making," *The McGraw-Hill Handbook of Homeland Security*, David Kamien, Editor.

Paul, R., Niewoehner, R. and Elder, L. 2006. *The thinker's guide to engineering reasoning*. Dillon Beach, CA: The Foundation for Critical Thinking.

Saari, D.G. 1999. Bad decisions: experimental error or faulty decision procedures?, Invited tutorial presented at the 1999 ASME meeting (Las Vegas, NV).

Tufte, E. R. 2006. *Beautiful evidence*. Cheshire, CT: Graphics Press, LLC.

Tversky, A. and Kahneman, D. 1999. Advances in prospect theory: cumulative representation of uncertainty. *Journal of Risk and Uncertainty* 5: 297-323.

U.S. Department of Defense. 2005. Department of Defense Directive 3020.40: Defense Critical Infrastructure Program (DCIP). Washington, DC: Office of the Assistant Secretary of Defense for Homeland Defense.

———. MIL-STD-1629A Notice 2. 1984. Procedures for performing a failure mode, effects and criticality analysis. Washington, DC.

U.S. Department of the Navy. 2004. Chief of Naval Operations Instruction 3500.39B: Operational Risk Management (ORM). Washington, DC: Office of the Chief of Naval Operations.

U.S. Government Accountability Office. 2008. DHS risk-based grant methodology is reasonable, but current version's measure of vulnerability is limited. GAO-08-852 Homeland Security. Washington, DC.

BIOGRAPHIES

Edouard Kujawski is an associate professor in the Systems Engineering Department at the Naval Postgraduate School. His research and teaching interests include the design

and analysis of high reliability/availability systems, risk analysis, and decision theory. He received a PhD in theoretical physics from MIT, following which he spent several years in research and teaching physics. He has held lead positions at General Electric, Lockheed-Martin and the Lawrence Berkeley National Laboratory. He has contributed to the design of particle accelerators and detectors, space observatories, commercial communication systems, the Space Station, and nuclear power plants. He was a participant and contributor to the Lockheed Martin *LM21 Risk Management Best Practices* and the original *INCOSE Systems Engineering Handbook*. He is a member of the San Francisco Bay Area Chapter of INCOSE and has served on the board of directors.

Gregory Miller is a Lecturer of Systems Engineering at the Naval Postgraduate School in Monterey, CA. He teaches courses in C4ISR, weapons systems technology, sensor systems technology, software engineering, engineering project management, and systems engineering and architecting. He received a BSEE from USNA and a MSEE from NPS. He has an extensive background in ship system life cycle engineering and acquisition. He has had several waterfront industrial tours managing U.S. warship maintenance, repair and modernization. He served as lead system engineer for the Submarine Electronic Warfare Support Measure In-Service Engineering Activity at NISE West in San Diego. He was also the Assistant Program Manager for Shore Networks in the Naval Integrated Networks program office at PEO (C4I) where he was responsible for providing executive-level leadership for the acquisition of several joint C4I systems. He is a member of the Defense Acquisition Corps. He is a member of ASNE and INCOSE.