10th International Conference of the International Institute for Infrastructure Resilience and Reconstruction (I3R2)
20–22 May 2014
Purdue University, West Lafayette, Indiana, USA

A Multicriteria Methodology for Measuring the Resilience of Transportation Assets and Prioritizing Security Investments

M. S. Dojutrek and S. Labi
Department of Civil Engineering, Purdue University

J. Eric Dietz
Department of Computer and Information Technology and Purdue Homeland Security Institute, Purdue University

ABSTRACT

Transportation project prioritization uses performance measures that are related to the transportation asset, its operations, and its environment. However, in the state of practice, evaluation does not consider directly the likelihood of natural or man-made threats, the infrastructure resilience, or the consequences of the infrastructure damage in the event that the threat occurs. Thus, during the prioritization of investments, assets of low security do not receive the due attention they deserve. In defining security as the lack of risk of damage from threats due to inherent structure or functional resilience, this paper is based on the premise that the inclusion of security considerations in prioritization introduces a much needed element of robustness in investment prioritization However, the inclusion of investment security impacts leads to an increase in the number of performance measures for the investment evaluation. This paper presents a methodology to quantify the overall security level for an asset in terms of the environmental threats it faces, its resilience or vulnerability to damage, and the consequences of the infrastructure damage. The overall framework consists of the traditional steps in risk management, and this paper's specific contribution is in the part of the framework that measures the risk. This paper applies the methodology to a given set of assets by measuring the risk (security) of each asset and prioritizing security investments across multiple assets using multiple criteria analysis.

1. INTRODUCTION

Disasters can result in millions and even billions of dollars in damage. For example, Hurricane Sandy caused about $50 billion in damages, and the tsunami in Japan caused about $308 billion in damages (Porter, 2013; Ridgwell, 2011). Additionally, events such as the Paramount Boulevard Bridge accident in California cost $40 million in damages and repair, and the Leo Frigo Memorial Bridge Pier failure cost $20 million in investigation and repair costs (Tata, 2012; Phelps, 2013). The occurrence and magnitude of these unexpected natural or man-made disasters cannot be predicted with absolute certainty; however, if civil infrastructure systems can be made to withstand better the potential damage resulting from these disasters, the consequences and costs of repair may be reduced.

Similar to all civil infrastructure systems, transportation assets encounter end-of-life situations when they face intended or unintended agents that cause their destruction. Unintended termination can be caused by the failure of the asset itself due to factors including design flaws, fatigue, advanced deterioration, and other internal causes, or due to external agents such as overloading, accidents, or natural events. Intended end-of-life events include deliberate retirement due to structural or functional obsolescence, terrorism, or vandalism. In any given jurisdiction, there is a wide range of types of threats to transportation infrastructure; however, if such threats to each asset can be identified and if the expected reduction in the asset damage due to security-enhancing investments can be predicted, then the reduction in the consequences of disaster can be forecast for each type of level of the security investment. When infrastructure is made resilient through security investments, the consequences of unintended end-of-life events can be reduced and the infrastructure itself can play a role in mitigating or recovering from the damage resulting from the event.

There are five key steps to risk management that should be considered to develop evidence for security investments (Ezell, Farr, Wiese, 2000):

- *Measure* the threat likelihood posed by external or intentional threats to the asset
- *Monitor* the threat likelihood over time
- *Assess* the effectiveness of actions intended to reduce consequences

- *Communicate* this information to the general public and legislators
- *Provide* evidence for appropriate resources

With the listed series of steps, a methodology to quantify security enhances the list to ensure security is of equal importance with respect to other performance measures and further plays a key role in determining asset prioritization for security funding.

Of the five key steps in risk management for reducing the overall negative impacts of transportation infrastructure damage, the first step is to measure the threat likelihood posed by forces external to the asset. If historical data such as earthquake occurrence or flooding tendency are available, then (1) these threat probabilities can be calculated to identify the areas of high threat likelihood, (2) the threat likelihood can be monitored over time to identify the optimal time of intervention, and (3) the effectiveness of asset improvements can be assessed in terms of the extent to which they can reduce the adverse consequences if the threat does occur. The fourth step involves communicating the gathered information to serve as support material for requesting funding purposely for investments geared toward securing the infrastructure from damage. With these steps, a case can be made to help improve transportation infrastructure in terms of security.

Furthermore, due to the uncertain nature of threats (their occurrence and magnitudes cannot be predicted with complete certainty [Dojutrek, 2014]), it is vital to incorporate concepts of uncertainty in any analysis that deals with risk prediction and security investment evaluation. Failure to consider uncertainty can lead to overestimation or underestimation of the likelihood of the threat, damage to the infrastructure, and consequences of the damage to the community. Uncertainty can be quantified by analyzing historical data trends and developing models for threat likelihoods and magnitudes, infrastructure damage due to the threat, resilience enhancement due to the security investments, and community consequences of threat occurrence.

At the current time, the funding allocation processes for transportation infrastructure at most agencies utilize performance measures that include the expected change in asset condition or remaining life, land use, air quality, connectivity, and so on. However, the impacts of competing investments on asset security are rarely considered in a direct manner. Thus, for assets that are located in an area of high threat likelihood, their respective proposed investments could help reduce the potential for infrastructure damage (and the consequent adverse impacts on the community). Current evaluation processes do not account for such beneficial impacts of the investments. As such, it is reasonable to argue that a performance measure that quantifies the security benefits (reduction of infrastructure damage risk due to external threats) should be considered in transportation investment evaluation and prioritization in general.

2. A REVIEW OF PAST WORK

Threat, vulnerability, and consequence information are important in risk assessment. Risk management includes a specification of which protective measures must be undertaken based on an agreed upon risk reduction strategy. The security industry has been slow to use measurable factors in reducing risk because of difficulties in establishing security-related metrics. As such, in the security industry, the most widely-used approaches to analyze risks are qualitative in nature in a bid to ensure that the lower-valued assets receive due consideration during the evaluation process. Typically, qualitative assessment assigns relative values to specific assets based on factors such as the criticality of loss or replacement costs. The threats against assets are also given a relative value based on the probability of taking place. The result is a risk equation that computes risk as a function of impact and likelihood of occurrence. The goal of a security design strategy should be the logical and incremental "buy down" of security risk so as to provide acceptable levels of protection for transportation agency assets and operations on a continuing basis (SAIC & PB Consult, 2009).

The American Association of State Highway and Transportation Officials (AASHTO) Vulnerability Assessment method is a guide developed specifically for transportation agencies to establish a vulnerability assessment method based on AASHTO's guidelines. The methodology focuses on subjectively assigning values to factors associated with asset criticality and vulnerability. Asset criticality and vulnerability scores are transformed into X and Y coordinates, respectively, and plotted to determine asset importance. Examples of criticality factors range from Deter/Defend Factors to Consequence to General Public Factors (AASHTO, 2002). Assets are then prioritized based on the subjective values assigned to each factor using the equation below.

$$Criticality\ Coordinate\ (X) = \left(\frac{x}{C_{max}}\right) \cdot 100$$

Where x is the total criticality score for asset n, and C_{max} is the highest criticality score attainable.

Vulnerability in the AASHTO vulnerability assessment is broken into three factors: Visibility and Attendance, Access to the Asset, and Site Specific Hazards (AASHTO, 2002). Each factor is broken into two subfactors and again given subjective values on a scale of one to five. The subfactors for each main factor are then multiplied together, and those results are added together as seen in the equation below.

$$Vulnerability\ Factor\ (y) = (A \cdot B) + (C \cdot D) + (E \cdot F)$$

Where *A* and *B* are subfactors of Factor 1, *C* and *D* are subfactors of Factor 2, and *E* and *F* are subfactors of Factor 3.

A vulnerability coordinate is derived for each asset using the equation below.

$$Vulnerability\ Coordinate\ (Y) = \left(\frac{y}{V_{max}}\right) \cdot 100$$

Where V_{max} is the highest attainable vulnerability score and *y* is the vulnerability total score for asset *n*.

The assets are then plotted in the coordinate system seen in Figure 1 and assets falling in Quadrant 1 of the graph are labeled high priority.

In Figure 1, the Consequence Assessment is assumed on the basis of the X and Y coordinates and their factors and subfactors. The method continues by listing possible countermeasures broken down into countermeasure functions of deter, detect, and defend to be considered for the assets that fall in Quadrant 1. Again, choosing countermeasures is a subjective process based on the countermeasure functions and decision maker. Finally, the countermeasures listed are assigned rankings of high, medium, or low.

The above-explained AASHTO methodology for risk management is quite subjective and uses surveys to obtain data (Venna & Fricker, 2009). Additionally, vulnerability and criticality are the only major factors that are included in the method to determine asset security importance, other important considerations, such as the resilience of the infrastructure, are not considered. Further, the method defines vulnerability and criticality as separate entities; however, one could argue that the concepts are not independent: if an asset is vulnerable then it has high criticality, and vice versa.

The CARVER + Shock methodology identifies seven vulnerability factors (criticality, accessibility, recoverability, vulnerability, effect, recognizability, and shock) and subjectively assigns a value on a scale of zero to ten to each, then the overall score is calculated as the sum of the scores assigned to the seven criteria (NIICIE, 2007). It accounts for target components of the target system and is applicable to features outside of transportation. This methodology is popular as local governments seek to leverage simple analysis tools to derive security-related information. It provides a “quick and dirty” means to rank potential targets based on vulnerability.

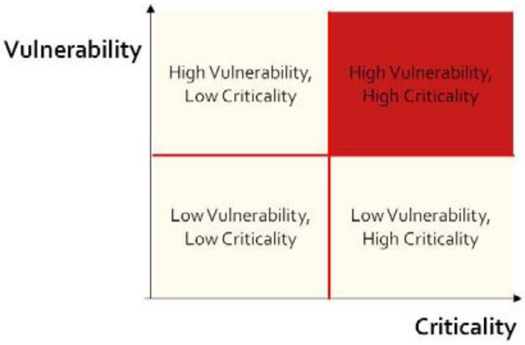

Figure 1. AASHTO vulnerability assessment chart

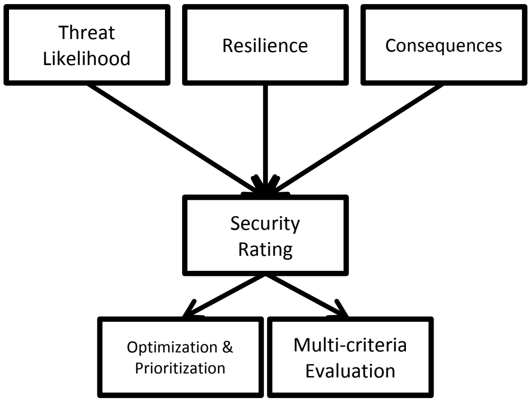

Figure 2. Proposed methodology framework

However, McGill and Ayyub (2007) pointed out that its additive and inherently nonprobabilistic nature does not produce results that can support security risk assessment.

The Costing Asset Protection for Transportation Agencies (CAPTA) method identifies security-related countermeasures for assets on the basis of the extent of potential losses (SAIC & PB Consult, 2009). CAPTA uses a consequence-based methodology that supports capital budgeting and resource allocation. The main purpose of the method is to reduce risks to a level manageable by operating agencies based on their available budget and resources. Consequence thresholds are established subjectively for the risk factors that include the potentially exposed population, property loss, and mission disruption. This method is mainly a decision informing tool for capital budgeting, not necessarily an asset specific assessment tool for prioritizing assets (SAIC & PB Consult, 2009).

3. METHODOLOGY

The proposed security rating developed in this study has three main inputs: Threat Likelihood, Resilience, and Consequence. The output is a security rating index which will be used to help in prioritizing assets for optimal security enhancement funding and used in multicriteria evaluation (Figure 2 [Dojutrek, 2014]).

Table 1. Terminology for methodology

Risk Factors	Term	Definition
Asset	*Target*	Transportation asset that has value to the owner or users
	Resilience	The ability of the asset to withstand the threat
Threat	*Threat*	An unexpected natural, unintentional man-made or intentional man-made event that causes damage or disruption
	Threat Likelihood	The probability that the threat occurs
Consequ-ence	*Consequence*	The loss of an asset and the effect of such loss to the community

The definitions of the key inputs and terminology used in the paper are defined in Table 1 (Dojutrek, 2014). Each of the three main factors, Threat Likelihood, Resilience, and Consequence, have measures that quantify how much the factor contributes to asset security. Each measure is further broken into attributes that indicate the level of the measure rated on a scale to define the overall amount that the measure contributes to the factor (Dojutrek, 2014). Since the attributes of each measure have different units, the attribute data was scaled to account for these differences.

Each risk factor follows the formulation below:

$$F_f = w_1 \cdot M_1 + \cdots + w_n \cdot M_n$$

f = 1….f

n = 1…n

Where F_f is a risk factor for the transportation asset, w_n is the weight/importance of measure *n*, and M_n is a measure of risk factor F_f.

Each measure of a risk factor follows the formulation below:

$$M_n = \frac{s_1 \cdot \ldots \cdot s_s}{N_s}$$

Where M_n is a measure of risk factor F_f; s_s is an attribute that contributes to the level of measure M_n, rated on a scale to define the overall amount that measure *n* contributes to the risk factor, F_f, and N_s is the number of attributes associated with measure *n*.

The security rating function can take any one of several forms. For example, addition, subtraction, multiplication, or ratio. Also, there are several ways by which they can be weighted. For purposes of this study, the security rating equation is shown below.

$$SR_a = \frac{F_{R_a}^{\alpha}}{\left(F_{TL_a}^{\delta} + F_{C_a}^{\lambda}\right)}$$

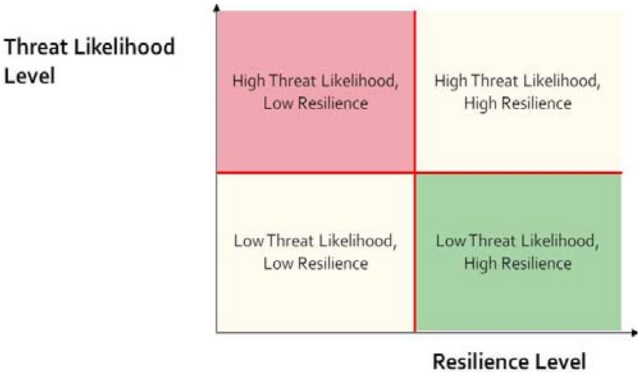
Threat Likelihood Level
High Threat Likelihood, Low Resilience
High Threat Likelihood, High Resilience
Low Threat Likelihood, Low Resilience
Low Threat Likelihood, High Resilience
Resilience Level

Figure 3. Threat likelihood factor versus resilience factor

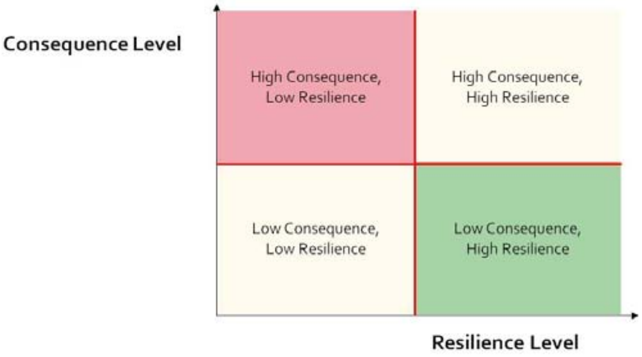
Consequence Level
High Consequence, Low Resilience
High Consequence, High Resilience
Low Consequence, Low Resilience
Low Consequence, High Resilience
Resilience Level

Figure 4. Consequence factor versus resilience factor

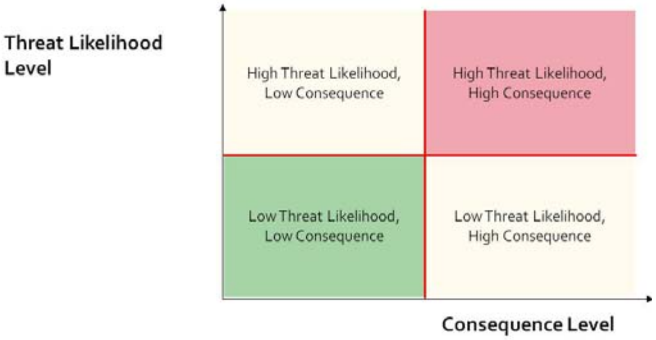
Threat Likelihood Level
High Threat Likelihood, Low Consequence
High Threat Likelihood, High Consequence
Low Threat Likelihood, Low Consequence
Low Threat Likelihood, High Consequence
Consequence Level

Figure 5. Threat likelihood factor versus consequence factor

Where SR_a is the Security Rating for asset *a*, F_{TLa} is the threat likelihood factor of asset *a*, *α* is the exponential weight of the resilience factor, F_{Ca} is the consequence factor of asset *a*, *δ* is the exponential weight of the threat likelihood factor, F_{Ra} is the resilience factor of asset *a*, and *λ* is the exponential weight of the consequence factor.

As asset resilience increases and threat likelihood and consequences decrease, the security rating increases. The greater the security rating, the more secure the asset is. Each factor can be graphed against each other to identify assets of importance as shown in Figures 3, 4, and 5.

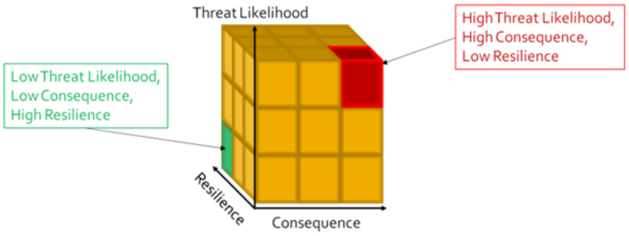
Threat Likelihood
High Threat Likelihood, High Consequence, Low Resilience
Low Threat Likelihood, Low Consequence, High Resilience
Resilience
Consequence

Figure 6. 3-D representation of security rating factor

Figure 7. JFK Bridge, Jeffersonville, Indiana

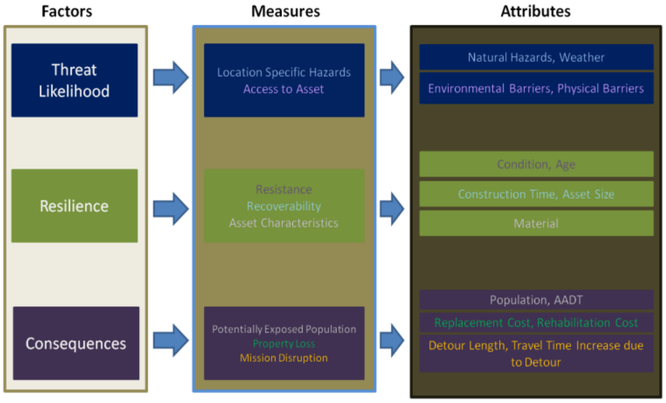

Figure 8. Detailed framework for case study

Additionally, a three-dimensional representation can also be derived from the three factors to show their interactions (Figure 6).

4. CASE STUDY

To demonstrate the study methodology, the National Bridge Inventory structure nr. 8868, the JFK Bridge in Jeffersonville, Indiana, was used (Figure 7).

The factors, measures, and attributes used for the case study are described in Figure 8.

The case study incorporated a number of assumptions. First, the construction time was based on the bridge size. Second, earthquakes were identified as the threat, and the probability of earthquake threat was equal to the amount of historical earthquake epicenters found in the county of location. Third, environmental barriers were assumed to be the waterway under the bridge. The detour travel speed was assumed to be 45 mph, and all weights in the security rating equation (α, δ, λ) and in the risk factor equations were assumed to be equal.

Table 2. JFK Bridge threat likelihood factor data

Measure	Attributes	Data	Scaled	Results
Access to Asset	Env Barriers	Over river	3	4.5
	Physical Barriers	Roadway underneath	3	
Location Specific Hazards	Natural Hazards	Earthquake epicenter	1	1.67
	County Freeze Index	30	1	
	County Precipitation	45.84	5	

Table 3. JFK Bridge resilience factor data

Measure	Attributes	Data	Scaled	Results
Resistance	Condition	Deck: 6	2	12
		Superstructure: 5	3	
		Substructure: 6	2	
	Age	83 yrs	4	
Recoverability	Const. Time	2yrs	4	41.67
	Const. Cost	$45.2M	5	
	Asset Size	267,466 ft^2	5	
Asset Characteristics	Material	Continuous steel	3	3.5
	Design Type	Truss Bridge	4	

Threat likelihood measures, attributes, and scales can be seen in Table 2.

$$F_{TL} = 0.5 \cdot 3 + 0.5 \cdot 2.33 = 2.67$$

Where F_{TL} is the threat likelihood risk factor.

The threat likelihood factor was calculated to be 2.67. The resilience measures, attributes, and scales are listed in Table 3. The resilience factor was calculated to be 19.2.

$$F_R = 0.33 \cdot 12 + 0.33 \cdot 41.67 + 0.33 \cdot 3.5 = 19.2$$

Where F_R is the resilience risk factor.

The consequence measures, attributes, and scales are listed in Table 4. The consequence factor was calculated to be 4.29.

Table 4. JFK Bridge consequence factor data

Measure	Attributes	Data	Scaled	Results
Potentially Exposed Population	Population	Jeffersonville: 27,362 Clark County: 96,472	3	3
	AADT	15,200	2	
Property Loss	Replacement Cost	$36.1M	4	8
	EDMC Value	$18.63M	4	
Mission Disruption	Detour Length (miles)	3.11	2	2
	Inc in travel time due to detour	4.15 min	2	

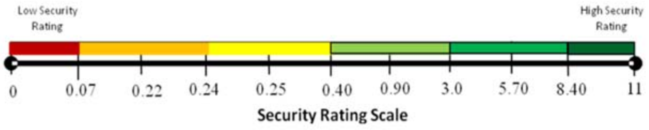

Figure 9. Tentative security rating scale

Table 5. Interpretation of security rating

Security Rating	Example Interpretation
≤ 0.21	Indicates a great need for security improvement of the asset. The asset has generally very low security thus immediate action should be undertaken to enhance its resilience and thus to reduce the possible consequences of threats.
0.25 – 0.21	Indicates significant need for security improvement needs of the asset. For this asset, the agency should be poised to undertake actions in the very near future, to enhance resilience and thus to reduce possible consequences of the asset failure.
0.40– 0.25	Indicates medium-to-high security improvement needs. Facilities within this range can be monitored at a frequency slightly exceeding standard frequency. The risk of failure can be tolerated until a normal capital project (to enhance resilience and thus reduce consequences, among other benefits) is carried out.
0.95– 0.40	Indicates low-to-medium security improvement needs. Unexpected failure can be avoided during the remaining service life of the asset by performing standard scheduled inspections with due attention to specific design features that influence the assets possible consequences.
3.03– 0.95	Indicates low security improvement need. Often reflective of the likelihood of threat to a civil engineering system built to the current design standards in a low threat likelihood environment.
11–3.03	Indicates little or zero security improvement needs.

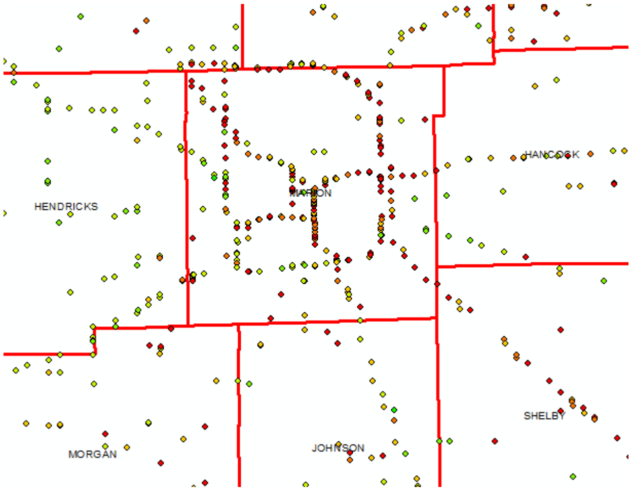

Figure 10. Spatial representation of overall risks for a section of Indiana bridges using security rating

$$F_C = 0.33 \cdot 3 + 0.33 \cdot 8 + 0.33 \cdot 2 = 4.29$$

Where F_C is the consequence risk factor.

The overall Security Rating of the JFK Bridge is then 3.03, which indicates a security rating of “medium”:

$$SR_{JFK} = \frac{19.2^1}{(2.67^1 + 4.29^1)} = 2.76$$

The security rating can be placed on a tentative scale and interpretations made, as seen in Figure 9 and Table 5.

Spatial analysis can be carried out to further enhance visualization of the security rating (see Figure 10, produced using GIS ArcMap 10.1).

5. SECURITY INVESTMENT AND PRIORITIZATION

Multicriteria decision making uses any of several alternative methods, including cost effectiveness, economic efficiency, the factor rating method, or the analytic hierarchy process. The cost effectiveness can be measured in terms of the increase in security rating or postproject security rating due to a security investment (Dojutrek, 2014). Economic efficiency can be calculated using the net present value, present worth of costs, or the benefit cost ratio. The factor rating method ranks different criteria based on subjective weighting. The analytic hierarchy process uses matrix multiplication of criteria weights to each alternative weight to derive the best option.

The evaluation criteria for security investment involve certain specific considerations. Effectiveness can be measured by increased infrastructure resilience and/or decreased consequences (Dojutrek, 2014). Costs can be measured in terms of agency costs (damage costs and repair costs) and user costs (travel time increase and detours). To measure security, the security rating described in this paper can be used for infrastructure as is, as an increase in security rating after security improvements and as a final security rating after improvements have been done (Dojutrek, 2014).

To incorporate the security rating into multicriteria evaluation as a performance measure, the security rating can be used for the asset in its current state as a generic performance measure that is the same for each project alternative (Table 6), as an "increase in security rating" that is alternative-specific and different for each proposed improvement (Table 7), and as a "final security rating" which is again alternative-specific and based on the enhancement to security that the improvement provides (Table 8). Each of these methods will prioritize security improvement alternatives based on the specific performance measure chosen.

The existing security rating prioritization indicates assets with low security rating scores to be of high importance and, therefore, in need of improvements. In the example in Table 6, Asset 2, with the lowest security rating, would be prioritized for further improvement needs.

The increase in security rating prioritization indicates the asset and associated alternative improvement with the greatest increase in security for an asset. In the example in Table 7, Asset 2 would be the most beneficial choice because of the alternative's high increase in security rating for the asset.

The final security rating prioritization indicates the asset and alternative with the greatest security rating after an improvement. In the example in Table 8, Asset 3 would be the alternative that gives the overall highest security rating after improvement.

Additionally, security can be incorporated into multicriteria evaluation by including security as one of the various performance measures used to evaluate transportation infrastructure. Example performance measure criteria are listed below.

Traditionally, the performance measures that are used in evaluation include: air quality, noise, economic efficiency, economic development, travel time, safety, vehicle operating cost, and connectivity. This paper argues that it is feasible and reasonable to add security as one of the multiple criteria in transportation investment evaluation, prioritization, and decision making. Secondly, for transportation investments specifically geared towards security enhancement, the framework presented in this paper could be used; for doing this, both the costs and the benefits (or effectiveness, in terms of the security rating increase) of the security project should be estimated. This paper addressed the benefits perspective.

Table 6. Simple example of existing security rating prioritization

Asset	Existing Security Rating (ESR)	Priority Rank on the Basis of Existing Security Rating
Asset 1	3.22	2
Asset 2	**2.45**	**1**
Asset 3	5.65	3
Asset 4	7.40	5
Asset 5	10.23	6
Asset 6	6.89	4

Table 7. Simple example of increase in security rating prioritization

Asset	Improvement	ESR[1]	ISR[1] (ΔSR)	Rank of ESR	Rank of ISR
Asset 1	Bridge Deck Overlay	3.22	4.57	2	4
Asset 2	**Bridge Substructure Maintenance**	2.45	**8.30**	1	**1**
Asset 3	Bridge Rehabilitation	5.65	7.22	3	2
Asset 4	Bridge Painting	7.40	0.52	5	6
Asset 5	Added Travel Lane on Bridge	10.23	1.32	6	5
Asset 6	Bridge Superstructure Replacement	6.89	4.88	4	3

[1]ESR: Existing Security Rating; ISR: Increase in Security Rating

Table 8. Simple example of final security rating prioritization

Asset	Improvement	ESR	ISR (ΔSR)	FSR (SR + ΔSR)	Rank of ESR	Rank of ISR	Rank of FSR
Asset 1	Bridge Deck Overlay	3.22	4.57	7.79	2	4	6
Asset 2	Bridge Substructure Maintenance	2.45	8.30	10.75	1	1	4
Asset 3	**Bridge Rehabilitation**	5.65	7.22	**12.87**	3	2	**1**
Asset 4	Bridge Painting	7.40	0.52	7.92	5	6	5
Asset 5	Added Travel Lane on Bridge	10.23	1.32	11.55	6	5	3
Asset 6	Bridge Superstructure Replacement	6.89	4.88	11.77	4	3	2

6. CONCLUSION

Prioritization of transportation assets typically utilizes performance measures related to asset characteristics, operations, and surrounding environment. The environmental criteria generally do not take into consideration asset security which can be stated as a function of the likelihood and magnitude, resilience of the transportation asset, and the resulting consequence in the event of the treat. Therefore, low security assets do not receive the due consideration they deserve during project prioritization. This paper presented a methodology to quantify the overall security level for an asset, using a case study, in terms of the threat likelihood, system resilience, and consequences in the event of system destruction or damage due to the threat occurrence. The paper's methodology addresses the risk measurement aspect of the traditional risk management framework. The paper applies the methodology to measure the security of a prominent transportation asset in Indiana. Finally, the paper shows how security rating can be used in multiple criteria investment evaluation for multiple assets.

REFERENCES

American Association of State Highway and Transportation Officials' Security Task Force. (2002, May). *A guide to highway vulnerability assessment for critical asset identification and protection* [PDF]. Vienna, VA: Science Applications International Corporation. Retrieved from http://highwaytransport.transportation.org/Documents/NCHRP_B.pdf

Dojutrek, M. S. (2014). *A stochastic multi-criteria assessment of transportation security investment*. (Unpublished doctoral dissertation). West Lafayette, IN: Purdue University.

Ezell, B. C., Farr, J. V., & Wiese, I. (2000). Infrastructure risk analysis model. *Journal of Infrastructure Systems, 6*(3), 114–117. http://dx.doi.org/10.1061/(ASCE)1076-0342(2000)6:3(114)

McGill, W. L., & Ayyub, B. M. (2007). Multicriteria security system performance assessment using fuzzy logic. *Journal of Defense Modeling and Simulation: Applications, Methodology, Technology*, *4*(4), 1–21. http://dx.doi.org/10.1177/154851290700400405

National Infrastructure Institute Center for Infrastructure Expertise. (2007). *CARVER2: Critical infrastructure assessment tool* [PDF]. Retrieved from http://knot9133.eti.pg.gda.pl/zl/infr_krytyczne/CARVER2demo.pdf

Phelps, N. (2013, November 10). Leo Frigo closure costing about $139,000 per day in travel delays. *Green Bay Press Gazette.* Retrieved from http://www.greenbaypressgazette.com/article/20131109/GPG0101/311090331/

Porter, D. (2013, February 12). Hurricane Sandy was second-costliest in U.S. history, report shows. *Huffington Post*. Retrieved from http://www.huffingtonpost.com/2013/02/12/hurricane-sandy-second-costliest_n_2669686.html

Ridgwell, H. (2011, March 24). Japan tsunami damage cost could top $300 billion. *Voice of America*. Retrieved from http://www.voanews.com/content/japan-tsunami-estimated-costliest-ever-disaster-118644489/137021.html

Science Applications International Corporation, & PB Consult. (2009). *Costing asset protection: An all-hazards guide for transportation agencies (CAPTA)* (NCHRP Report 525). Surface Transportation Security, 15. Washington, D.C.: Transportation Research Board. Retrieved from http://www.trb.org/Main/Blurbs/160337.aspx

Tata, S. (2012, February 28). 60 freeway in Montebello to close for bridge demolition. *NBC4 Southern California*. Retrieved from http://www.nbclosangeles.com/news/local/60-Freeway-Bridge-to-Close-For-Demolition-Montebello-Pomona-140664893.html

Venna, H. R., & Fricker, J. D. (2009). *Synthesis of best practices in transportation security, volume I: Vulnerability assessment*. Publication FHWA/IN/JTRP-2007/19-I. West Lafayette, IN: Joint Transportation Research Program, Indiana Department of Transportation and Purdue University. http://dx.doi.org/10.5703/1288284314236