On decision optimality of terrorism risk mitigation measures for iconic bridges

Thöns, Sebastian; Stewart, Mark G.

Published in:
Reliability Engineering & System Safety

Link to article, DOI:
10.1016/j.ress.2019.03.049

Publication date:
2019

Document Version
Peer reviewed version

On Decision Optimality of Terrorism Risk Mitigation Measures for Iconic Bridges

Sebastian Thöns , Mark G. Stewart

PII: S0951-8320(18)30448-4
DOI: https://doi.org/10.1016/j.ress.2019.03.049
Reference: RESS 6442

To appear in: *Reliability Engineering and System Safety*

Received date: 9 April 2018
Revised date: 19 March 2019
Accepted date: 28 March 2019

Please cite this article as: Sebastian Thöns , Mark G. Stewart , On Decision Optimality of Terrorism Risk Mitigation Measures for Iconic Bridges, *Reliability Engineering and System Safety* (2019), doi: https://doi.org/10.1016/j.ress.2019.03.049

HIGHLIGHTS

- Utilization of the Bayesian probability, utility and decision analysis
- Consistent assessment of information acquirement and physical mitigation strategies
- Identification of optimal, significant and efficient strategies before implementation

On Decision Optimality of Terrorism Risk Mitigation Measures for Iconic Bridges

Sebastian Thöns

Technical University of Denmark, Lyngby, Denmark

Mark G. Stewart

The University of Newcastle, New South Wales, Australia

ABSTRACT: This paper describes the assessment of the cost efficiency of risk mitigation strategies for terrorist attacks with Improvised Explosive Devices (IEDs) for an iconic bridge structure. The assessment is performed with a decision theoretical framework building upon very recent advances in the COST Action TU1402 on Quantifying the Value of Structural Heath Monitoring. The decision scenario is formulated for a decision maker constituting an authority responsible for the societal safety of the infrastructure and consequently the direct risks for the infrastructure owner and the indirect risk due to fatalities and importance of the infrastructure are considered. The mitigation strategies are classified within the decision theoretical context as prior analyses for the assessment of protection strategies and as control strategies requiring a pre-posterior decision analysis. The identification of efficient risk mitigation strategies is based (1) on the risk and expected cost based optimization of actions and information and their combination before implementation, (2) on quantifying and ensuring the significance in risk and expected cost reduction and (3) on quantifying and ensuring a high probability of cost efficiency. These criteria, i.e. the optimality, significance and efficiency ensure the performance of the strategies at the decision point in time before implementation. It is found that the strategies are relying on the identification of the threat level and that control strategies are in favor as their significance and probability of efficiency are higher and their costs are adjustable. However, for high threat levels, both the bridge protection strategies and control strategies are cost efficient.

1 INTRODUCTION

The study of protective measures and their efficiency for terrorist threats constitutes to society a very relevant and important topic of research and is challenged by the seemingly permanent terrorist threats and by risk-averse regulatory measures e.g. in US (e.g. [1], [2], [3], [4], [5] and [6]). The research on hazard and risk assessment of infrastructure systems has substantially increased in the last few decades. For example, methods for the investment optimization for unknown and emerging threats focused on infrastructures and on large scale networks [7], [8], the utilization of risk assessment approaches for the identification of critical US bridge infrastructures [9], and the identification of critical road network corridors [10] have evolved. Explosive loading scenarios have been comprehensively analyzed and modelled, see e.g. explosive loading and structural performance modelling in e.g. [4], [11], [12] and [13], the improvised explosive device performance (e.g. [14]), and the structural design for explosive loads [15].

The effectiveness of security measures for critical infrastructures based on utility and game theory is analyzed by Hausken [16] who focuses on the modelling and quantification of terrorist utilities benefitting from the

loss of human lives and loss of economic value. This game theoretical model is extended in [16], by introducing a governmental player who optimizes the security measure investments by maximizing its expected utility calculated as the product of threat score and a target valuation.

However, an efficient implementation of counter-terrorism strategies necessitates a forecast, an analysis and an optimization of the risk reduction by information acquirement strategies and risk mitigation measures before their implementation. This is facilitated by the utilization of the pre-posterior decision analysis based on the Bayesian probability, utility and decision theory. This paper thus focusses on (1) the explicit formulation of the optimization of risk mitigation strategies in the framework of the Bayesian probability, utility and decision analysis building upon [17], [18], [19] and (2) the combined and consistent assessment of the performance of information acquirement strategies with risk mitigation measures. The optimization will lead to the identification of efficient information acquirement and protective measures for terrorism risk reduction in the context of on long span and iconic bridges like e.g. the recently completed 2.7 km cable stayed Queensferry Crossing bridge near Edinburgh in Scotland with a cost £1.35 billion or $1.9 billion [20]; and the Golden Gate Bridge is valued today at approximately $1.6 billion [21]. It should be noted that for such infrastructure, a high (target) valuation of terrorists and of the government can be found in [16].

The decision theoretical approach is formulated in Section 2 distinguishing counter terrorism protection measures, which may be implemented in the design phase of a bridge, and control, i.e. information acquirement via surveillance, strategies and accordingly prior and pre-posterior decision analyses. The objective function for the calculation and optimization of the risk and the expected consequences and costs in dependency of the decision variables strategies and information and action parameters of strategies is formulated. Section 3 contains the description of the decision scenarios in the context of Improvised Explosive Device (IED) attacks to large iconic bridges and the development and discussion of the probabilistic information, information precision, action and system states and consequence models for the individual risk mitigation strategies. The results for the protection strategy and control optimization are shown in Section 4 and the optimal decision variables are explicated and explained. The paper concludes with a discussion of the boundaries of the analysis and insights gained beyond its specifics in Section 5 and with a summary and the conclusions in Section 6.

2 APPROACH

The approach of assessing information and protection measures for structures under terrorism attacks takes basis in the framework for structural integrity and risk management as developed in [22] and [23]. Figure 1 shows an adapted decision tree distinguishing a do-nothing (i.e. business as usual) branch and risk mitigation strategy branches with and without additional information. These main branches contain choice nodes (rectangles) for decision variables and chance nodes for probabilistic models associated to the choice nodes. Consequences are symbolized with diamond shapes nodes.

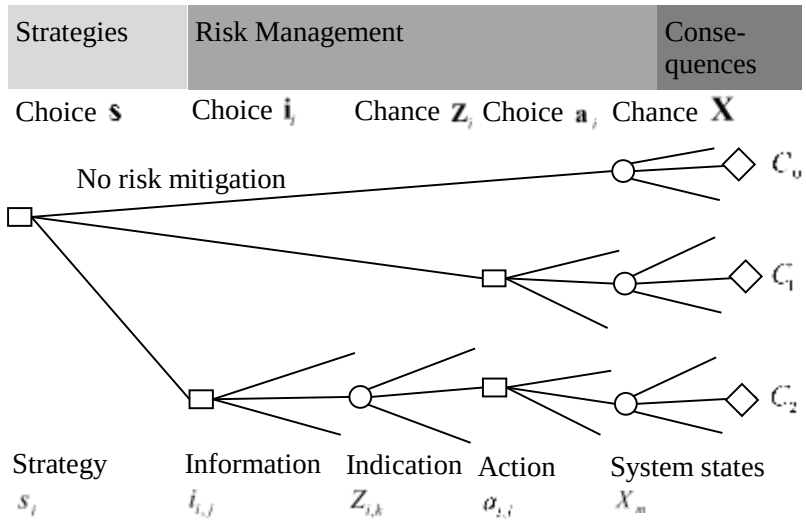

Figure 1: Decision tree for risk mitigation strategies with decision nodes (rectangles), change nodes containing the probabilistic models (circles) and consequence nodes (diamonds)

The decisions are based on the minimization of the expected value of the consequences in dependency of the choices, i.e. decision variables. The expected consequences for the strategies without and with additional information, $E\left[C_1\left(a_1^*\right)\right]$ and $E\left[C_2\left(i_2^*,\mathbf{a}_2^*\right)\right]$ respectively, are defined with the strategy s_1 optimal actions a_1^*, the strategy s_2 optimal set of actions $\mathbf{a}_2^*$ and the optimal information acquirement strategy i_2^*. The expected consequence in the do-nothing-branch is denoted with $E\left[C_0\right]$ and its system states with $X_m \in \mathbf{X}$.

The expected consequences with no consideration of additional information $E\left[C_1\left(a_1^*\right)\right]$ represent a prior decision analysis as they depend solely on the choice of actions $a_{1,l} \in \mathbf{a}_1$ and the - eventually action dependent - probabilistic system state models $X_m \in \mathbf{X}$:

$$E\left[C_1\left(a_1^*\right)\right] = \min_{a_{1,l} \in \mathbf{a}_1}\left(E_{X_m}\left[C_1\left(a_{1,l}, X_m\right)\right]\right) \tag{1}$$

The expected consequences with consideration of additional information $E\left[C_2\left(i_2^*,\mathbf{a}_2^*\right)\right]$ is dependent on the vector of information acquirement strategies $i_{2,j} \in \mathbf{i}_2$, their probabilistic outcome models $Z_{2,k} \in \mathbf{Z}_2$ and the strategy dependent set of actions and the system states. In the extensive form, the expectation over the posterior system states is calculated by Bayesian updating (operator E''_{X_m}) and the dependency on the system states is then marginalized with the expectation in regard to the probabilistic information outcomes with the operator $E_{Z_{i,k}}$:

$$E\left[C_2\left(i_{2,j}^*,\mathbf{a}_2^*\right)\right] = \min_{i_{2,j} \in \mathbf{i}_2} E_{Z_{2,k}}\left[\min_{a_{2,l} \in \mathbf{a}_2} E''_{X_l}\left[C_2\left(i_{2,j}, Z_{2,k}, a_{2,l}, X_m\right)\right]\right] \tag{2}$$

The value of the strategies may be expressed as the decrease in the expected value of the consequences due to the identification of the optimal action strategy or the optimal information acquirement and action strategy:

$$V_{s_1} = E\left[C_0\right] - E\left[C_1\left(a_1^*\right)\right] \tag{3}$$

$$V_{s_2} = E\left[C_0\right] - E\left[C_2\left(i_2^*,\mathbf{a}_2^*\right)\right] \tag{4}$$

For a positive strategy value, the optimal strategy is identified by maximizing the expected consequence decrease, which is equivalent to the minimization of the expected value of the consequences (Equ. (1) and (2)):

$$V = \max_{s_i}\left(V_{s_1}, V_{s_2}\right) \tag{5}$$

The measure of significance of these information acquirement and/or action strategies is defined with relating the expected consequence decrease to the expected consequence of the no mitigation base scenario:

$$\bar{V}_{s_1} = \frac{E[C_0] - E\left[C_1\left(a_1^*\right)\right]}{E[C_0]} \tag{6}$$

$$\bar{V}_{s_2} = \frac{E[C_0] - E\left[C_2\left(i_2^*, \mathbf{a}_2^*\right)\right]}{E[C_0]} \tag{7}$$

Beyond the identification of the optimal strategies on the basis of the expected value, the probabilistic characteristics of the consequence distributions C_0, $C_1\left(a_1^*\right)$ and $C_2\left(i_2^*, \mathbf{a}_2^*\right)$ should be considered (see Equ. (1) and (2)) to ensure that the risk mitigation strategies are cost efficient. With the distribution of the consequences, the probability of cost efficiency of information acquirement and/or action strategies can be calculated in relation to the base scenario of no risk mitigation, i.e. $P\left(C_1\left(a_1^*\right) > C_0\right)$ and $P\left(C_2\left(i_2^*, \mathbf{a}_2^*\right) > C_0\right)$.

3 DECISION SCENARIOS

In the following an iconic bridge with a value of €2.0 Billon or annual cost of €81 Million for a 100 year design life and an interest rate of 4% is considered. The decision maker is a public authority responsible for the safety of a large scale and iconic bridge. The objective of the decision maker is to minimize total risks for society and the bridge users and thus to implement mitigation strategies, which minimize the total risks and expected costs on an annual basis.

Two risk mitigation strategies are distinguished, namely, the implementation of protective measures in bridge design (strategy protect: s_1) and the implementation of a surveillance system in combination with bridge temporary closure during times of high threats (strategy control: s_2) taking basis in [1] and [24].

3.1 *System state model and consequences*

The system states safe and bridge collapse are analyzed. The probability of a collapse is calculated with the probability of a threat $P(T)$, the conditional probabilities of a hazard $P(H|T)$ and collapse of the bridge $P(F|H)$, i.e.:

$$P(F) = P(F|H) \cdot P(H|T) \cdot P(T) \tag{8}$$

The probability of threat can be inferred by looking back to past threats and hazards. However, current threat information should also be accounted for and the estimation of the threat probabilities should be based upon information by police and security services. Such information are usually not public nor accessible by scientists. It should further be considered that large and iconic bridges may attract attackers more than typical highway bridges and it may also attract skilled attackers so that the likelihood of an attack increases [1]. Thus,

e.g. in US the San Francisco's Golden Gate Bridge or New York's Brooklyn Bridge might be a more tempting target for terrorists as evidenced by the 2002 poorly conceived (and quickly abandoned) plot to sever the stay cables of the Brooklyn Bridge with blowtorches [39].

The quantification of the threat probability in the U.S. based on the publicly known plots would result in $6.7 \cdot 10^{-6}$ per bridge per year. The basis are the Brooklyn bridge plot as the only one in 15 years against a large bridge in the U.S. and 1000 large/iconic bridges in the U.S. [25]. The 2002 plot to destroy the Brooklyn Bridge was more fanciful than a serious threat. Mueller [26] summarizes the threat as "in 2002, Iman Faris travelled to New York City under orders from Khalid Sheikh Mohammed to survey possible terror targets within the United States. After basic internet research Faris decided on the Brooklyn Bridge as a potential target and believed that 'gas torches' could be used to bring the bridge down. However after conducting physical reconnaissance of the bridge (which consisted of driving over it once), Faris concluded that an attack was unlikely to succeed "because of the bridge's structural design and because of the New York Police Department patrols there, and he never sought to acquire the equipment necessary for such an attack." There may be other threats that we are unaware of, but the threat level is likely to be less than one threat per year. No plots are publically known to the authors in Europe.

The conditional probability of a hazard $P(H|T)$ may be assessed by considering the construction, placement and successful donation of an explosive device. While the technical reliability of an IED detonation is high [27], human errors play a significant role and reduce the probability of a successful attack. The past information for Western countries has been studied in [14] for the time period of 1970 to 2013. The analyses used two different measures for success; (i) non-attacker fatalities and (ii) non-attacker casualties and/or significant infrastructure damage (i.e. greater than $1 million in U.S. dollars), see Table 1.

Table 1: IED Attack Success Rates in Western Nations (adapted from[14])

	1970-2013		1970 – 1997		1998 - 2013		2002 - 2013
Location	Fatalities	Casualties or >$1 million infrastructure damage	Fatalities	Casualties or >$1 million infrastructure damage	Fatalities	Casualties or >$1 million infrastructure damage	Fatalities
Western Countries	8%	21%	9%	22%	4%	19%	3%
Great Britain	12%	-	-	-	-	-	13%
U.S.	3%	-	-	-	-	-	4%
Spain	9%	-	-	-	-	-	7%
Northern Ireland	21%	-	-	-	-	-	1%
Other Western Countries	4%	-	-	-	-	-	2%

Given that Northern Ireland and Spain sustained prolonged terror campaigns across the period 1970–2013, this table provides some context to the actual threat arising from IED Attack for relatively stable political environments (U.S. and Great Britain), and unstable political environments (Northern Ireland and Spain). Indeed, in the post-9/11 environment a general decline in the success of IED Attacks is observed, noting that for the U.S., Great Britain and Spain the number of attacks post-9/11 are biased by considering the Boston 2013, London 7/7 and Madrid 2004 bombings as numerous separate attacks [14]. Table 1 shows that $P(H|T)$ may

reach a maximum value of 22%, and an average 3% if success is based on attacks causing fatalities. If we assume that an iconic bridge may be attacked by skilled terrorists, a triangular distribution with a minimum of 0%, a mode of 15% and a maximum of 25% is utilized, see also [3].

The probability of a bridge collapse $P(F|H)$ depends on the scenario, i.e. the energy release of the IED charge, its location and the structural system and its robustness. The probability of a bridge collapse is assessed rather high to $P(F|H)=90\%$ due to (1) the assumption that an IED contains a large amount of explosives, (2) skilled terrorist are assumed having being able to design a collapse scenario and (3) iconic bridges may have a highly utilized structural system with a low redundancy. Studies of progressive collapse of e.g. cabled stayed bridges ([28] and [29]) point towards a high collapse probability for the assessed scenarios. Further, the need for more robust bridges is acknowledged and approaches can e.g. be found in [30].

The consequences of a bridge collapse encompass the property damage and reconstruction costs to the bridge structure and the vehicles on the bridge as the direct consequences and the costs from fatalities, the indirect costs linked to the importance of the bridge in the road network, traffic diversions and user delays, business losses, etc. Added to these are social losses that reflect the level of fear and anxiety within society (and perhaps on civil liberties). The losses are interconnected, for example, a fearful public may be reluctant to travel and so contribute to business and tourism losses, or may be reluctant to invest. People often effectively place a higher value on a life lost to terrorism than on one lost to more mundane and less sensational hazards [31]. A value of statistical life (VSL) approach concluded that the best estimate is about $7.5 million in 2015 dollars [32]. Most VSL studies focus on relatively common risks (e.g., workplace or motor vehicle accidents) and Robinson et. al. [32] suggest that 'more involuntary, uncontrollable, and dread risks may be assigned a value that is perhaps twice that of more familiar risks,' a process that essentially adds into the analysis much of the substantial indirect and ancillary costs associated with a terrorist event. The differentiation between direct, indirect, and social losses is less precise, hence, aggregate losses presented in this section tend to err on the conservative side by placing a high premium on indirect and social losses as "increased fear and anxiety within society may be one of the most important consequences of terrorist attacks" [32].

The Federal Highway Administration Blue Ribbon Panel on bridge and tunnel security found that the "loss of a critical bridge or tunnel at one of the numerous 'choke points' in the highway system could result in hundreds or thousands of casualties, billions of dollars worth of direct reconstruction costs, and even greater socioeconomic costs," that the "ordinary cost of construction to replace a major long-span bridge or tunnel on a busy interstate highway corridor in the United States may be $1.75 billion," and that, summing reconstruction costs and socioeconomic losses, the "loss of a critical bridge or tunnel could exceed $10 billion." [25]. The ratio of total loss to bridge replacement value is estimated to $10 billion/$1.75 billion = 5.7. This is a reasonable estimate as in [25] it is also stated that "the socioeconomic loss to the region resulting from losing as many as 14 Interstate highway lanes for an extended period is many times the replacement cost of the facility."

Based on EU project Security of Road Transport Networks (SeRoN: [24] and [33]), tons of explosives would be necessary to cause collapse of a 2-lane, 250 m concrete arch highway bridge. In this scenario, reconstruction cost is €43 million, fatalities is €160 million using a VSL of €6.3 million per person (i.e. $7.5 million), and €80 million for indirect losses – leading to a total loss of approximately €280 million. The bridge value is €30 million, leading to a loss to bridge replacement value of 9.3.

We can establish something of an upper bound by beginning with an estimate of the direct and indirect losses inflicted by the terrorist attack that has been by far the most destructive in history, that of September 11, 2001. The attack directly resulted in the deaths of nearly 3,000 people. Using a VSL of $7.5 million leads to a direct loss of approximately $25 billion arising from 3,000 fatalities. In addition 9/11 caused approximately $30 billion in physical damage including rescue and clean-up costs [34]. Indirect costs were even more substantial. Thus, the International Monetary Fund estimates that the 9/11 attacks cost the U.S. economy up to 0.7% in lost GDP ($125 billion in 2016 dollars) in that year alone, while others estimate that associated business costs and loss of tourism cost the U.S. economy $200 billion over three years (Hook 2008). Blomberg

and Rose [35] estimate that the impact on the U.S. economy of the 9/11 attacks range from 0.3 to 1% of GDP or $50-175 billion in 2017 dollars. An upper bound estimate of the losses of 9/11, then, might approach $250 billion. However, this sum is for the total losses inflicted by four hijacked aircraft, not one. The destruction of a long-span or iconic bridge is very unlikely to trigger the same public response as the 9/11 attacks. A high, upper limit would be a lower bound drop in GDP of say 0.3% that equates to $50 billion, loss of life (say 500 fatalities) equates to $3-4 billion, and reconstruction cost of $2-4 billion. In this case, the total losses are around $60 billion. The FHWA [25] $1.75 billion estimate to build a major long span bridge in 2003 equates to approximately $2.4 billion in 2017 dollars, hence, the loss to bridge replacement value equals 60/2.4=25. Following the above reasoning a Triangular distribution between 5 and 25 with a mode at 10 is herein used.

3.2 *Prior decision analysis: Protective measures in bridge design*

Measures to enhance security for new and existing bridges typically focus on strengthening columns and girders by fiber-reinforced polymers (FRPs), additional steel reinforcement, minimum dimensions, adding lateral bracing, and increasing stand-off by bollards, security fences, and vehicle barriers. Although there is much information available about design and retrofitting bridges to mitigate the effects of blast damage there is little information about their cost [1]. However, the FHWA Blue Ribbon Panel report [25] contains a cost analysis of protective measures for four large U.S. bridges, and concludes that the cost to protect these bridges ranges from $20.6 to $157.4 million. For an average cost of $95.6 million, and a 2003 bridge value of $1.75 billion, the cost to protect a bridge from terrorist attack is 5.5% of the total bridge value. We will assume that substantial mitigation of blast effects can be achieved for a new bridge at a cost of 5% of a bridge's replacement value. Annualized over a design life of 100 years at a 4% discount rates result in an annual cost of protection of 0.2%. We will generously assume that these protective measures reduce the risk by a substantial $\Delta R = 95\%$.

The EU project Security of Road Transport Networks [24] reports that strengthening the concrete of a 250 m arch highway bridge is less likely to damage the bridge in the event of an IED attack. In this case, strengthening the arch will increase construction costs by €1 million or 3.3% of the bridge value. This equates to an annual cost of 0.13% if discounted over 100 years at a 4% discount rate. The risk reduction is approximately 75% [24]. Based on the above argumentation, the risk reduction-cost-relationship (ΔR to C_{Prot}) in Figure 2 is established. The relationship implies that very high risk reduction measures may only be achieved with an over-proportional cost increase. Low to moderate risk reduction maybe achieved with an almost linear cost increase. It is noted that the risk reduction-cost-relationship follows the law of diminishing returns, i.e. protective measures that are at once effective and relatively inexpensive are generally the first to be implemented, and thus the first expenditures on counterterrorism protective measures are often more likely to be worthwhile - that is, to be cost-effective - than additional expenditures.

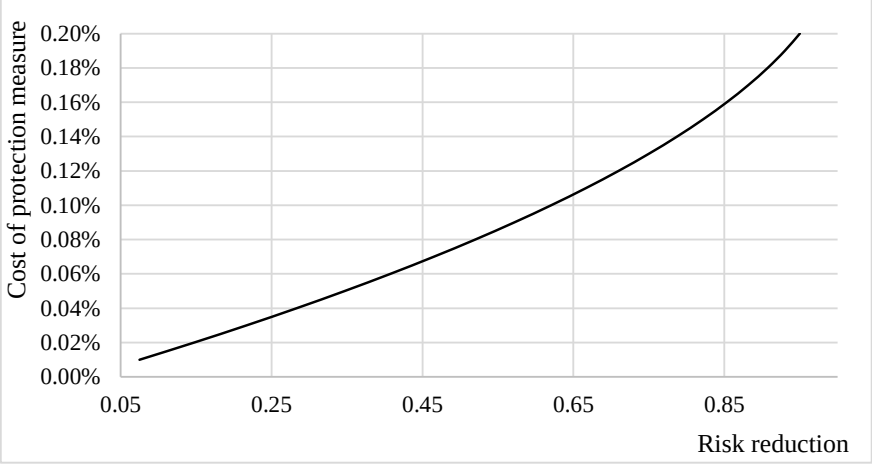

Figure 2: Costs of protective measure in dependency of their risk reduction performance.

The probabilistic model for the protection measure strategy is summarized in Table 2.

Table 2: Probabilistic model for the prior decision analysis on the cost efficiency of protective measures (strategy: protect s_1)

Nodes, states		Consequence model	Performance model
Do nothing	a_0	0	-
Protective actions	$\mathbf{a}_{1,1}$	$\mathbf{C}_{\text{Prot}} = [0.01 \ldots 0.2\%]$	$\Delta\mathbf{R} = [0.075 \ldots 0.95]$
Safe	X_0	0	$1 - P(F)$
Fail	X_1	Tr(25.0,10.0,5.0)	$P(F)$

Tr: Triangular distribution

3.3 *Pre-posterior decision analysis: Surveillance information and bridge closure*

A control strategy encompassing surveillance information in combination with bridge closure may be implemented in the design or in the operation phase of a bridge. The bridge closure would be required if surveillance information resulted in an imminent threat detection necessitating a temporal bridge closure to allow for time to apprehend the terrorists or defuse an IED.

The surveillance information are described with their detection performance, i.e. the indication and no-indication probabilities of threats in conjunction with the costs of the surveillance system investment and operation. The surveillance information model utilized here covers various strategies from enhanced incident detection (low costs as it may be integrated in the existing systems) to high cost systems with a high detection probability. The detection probability of surveillance systems can be assessed, see e.g. [36], [37], [38], [39], [40], [41]. Consequently, the indication probability given a threat and the no-indication probability given no threat, $P(\mathbf{Z}_{2,1} \mid T)$ and $P(\mathbf{Z}_{2,0} \mid \bar{T})$, respectively, are varied between 0.7 and 0.99 (Table 3). The posterior probabilities of bridge collapse $P''(F)$ according to Equ. (10) are calculated with the updated threat probability:

$$P(T \mid \mathbf{Z}) = \frac{P(\mathbf{Z} \mid T) \cdot P(T)}{P(\mathbf{Z} \mid T) \cdot P(T) + P(\mathbf{Z} \mid \bar{T}) \cdot P(\bar{T})} \tag{9}$$

$$\text{with } \mathbf{Z} = \left[\mathbf{Z}_{2,0}, \mathbf{Z}_{2,1}\right] \tag{10}$$

The rate of increase of annualized costs of the surveillance systems increases with a higher rate for precise systems as shown in Figure 3. The costs are taking basis in the investment, installation and operation cost with a 10 years replacement interval. A system with a low detection performance of 0.7 would require investment and installation costs of 20 k€ and operation costs of 6 k€ per year (similar to video surveillance costs in [24]). For a surveillance system with a detection rate of 0.97, the investment and installation cost sum up to 150 k€ with 46 k€ yearly operational expenses.

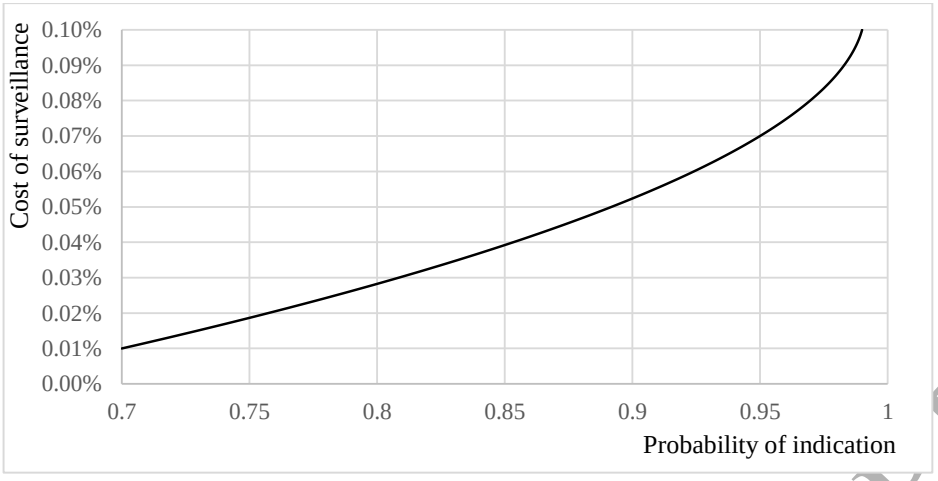

Figure 3: Costs of surveillance systems in dependency of their reliability.

The cost of the bridge closing are calculated with the bridge importance in the traffic network and the associated costs based on [24] and [33]. A bridge closure of 2 days is assumed for attack prevention and eventual explosive charge detection, location and deactivation activities leading to costs of 0.27% for the considered bridge. The bridge closure leads to a reduction of the consequences for bridge collapse by reduction of the property damage including a lower number of vehicles on the bridge and consequently a reduction of the costs due to fatalities, bridge reconstruction and traffic diversion. A Uniform distribution of total loss to bridge replacement value between 1.0 and 5.0 is assumed (Table 3).

Table 3: Probabilistic model for the pre-posterior decision analysis on the cost efficiency of surveillance information (strategy: control S_2)

Nodes, States		Consequence model	Performance model	
			T	$\bar{T}$
No threat indication	$\mathbf{Z}_{2,0}$	$\mathbf{C}_{\text{Surv}} = [0.01\ldots0.1\%]$	[0.3…0.01]	[0.7…0.99]
Threat indication	$\mathbf{Z}_{2,1}$		[0.7…0.99]	[0.3…0.01]
Do nothing	$a_{2,0}$	0	-	
Close bridge	$a_{2,1}$	0.27%	-	
Safe	X_0	0	$1-P''(F)$	
Fail	X_1	Tr(5.0,10.0,25.0)	$P''(F)$	
Fail given closure	$X_1 \mid a_{2,1}$	U(1.0,5.0)	$P''(F)$	

Tr: Triangular distribution, U: Uniform distribution

3.4 *Summary of strategies*

Figure 4 contains the decision tree for the analysis of the protection strategy with a prior decision analysis and the control strategy with a pre-posterior decision analysis. It should be noted that the branch $\mathbf{Z}_{2,0}: a_{2,1}$, i.e. bridge closure in case of a no threat indication, is excluded.

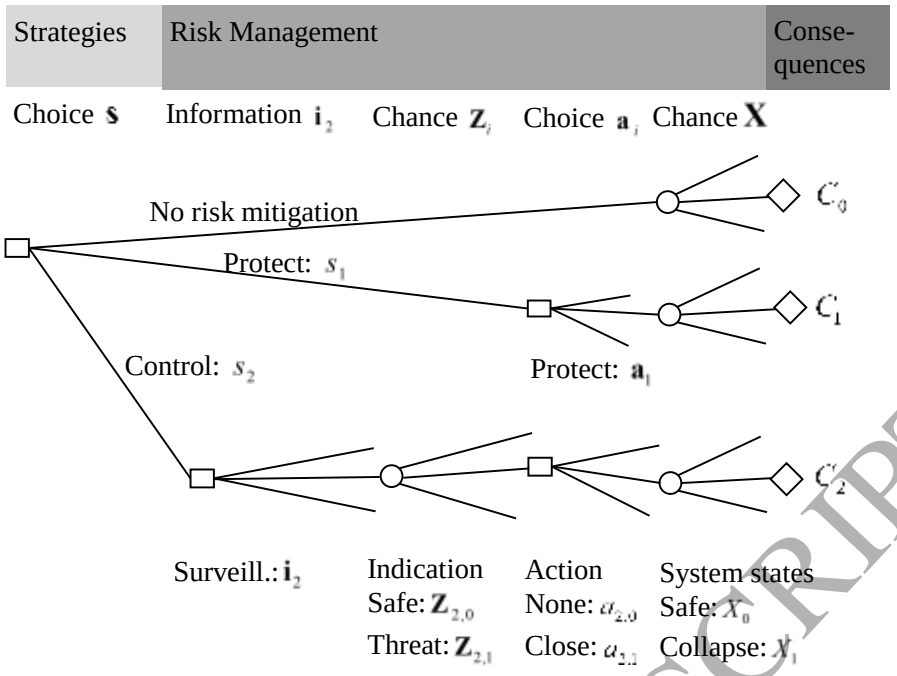

Figure 4: Decision tree for analyzed strategies

4 RESULTS

The established decision scenario is analyzed individually in detail for the protection strategy and the control strategy and then jointly by the explanation of the results and the identification of the optimal protection and/or control strategy on the basis of the minimum risk and expected costs, their significance and the probability that measures are cost efficient. The threat probabilities are chosen to illustrate the change in risk and expected costs from the optimal decision do-nothing to protection and/or control and thus the relevance of the significance and cost efficiency quantification.

4.1 *Analysis of protective measures*

The analysis and optimization of the protective measures is performed in dependency of the performance and the cost of the measures (see Figure 2) and for threat levels between $P(T) = 0.9 \cdot 10^{-3}$ and $P(T) = 2.0 \cdot 10^{-3}$ per bridge per year. Figure 5 shows the minimum risk and expected costs dependent on the protection risk reduction. A change of the optimal action results in a discontinuity of the curve, e.g. at $\Delta R = 86\%$ for an annual threat probability of $P(T) = 1.2 \cdot 10^{-3}$. Here, the optimal action changes from do-nothing to protection. For increasing threat levels, the change of the optimal action shifts towards protection measures with a higher risk reduction and the curves become more peaked.

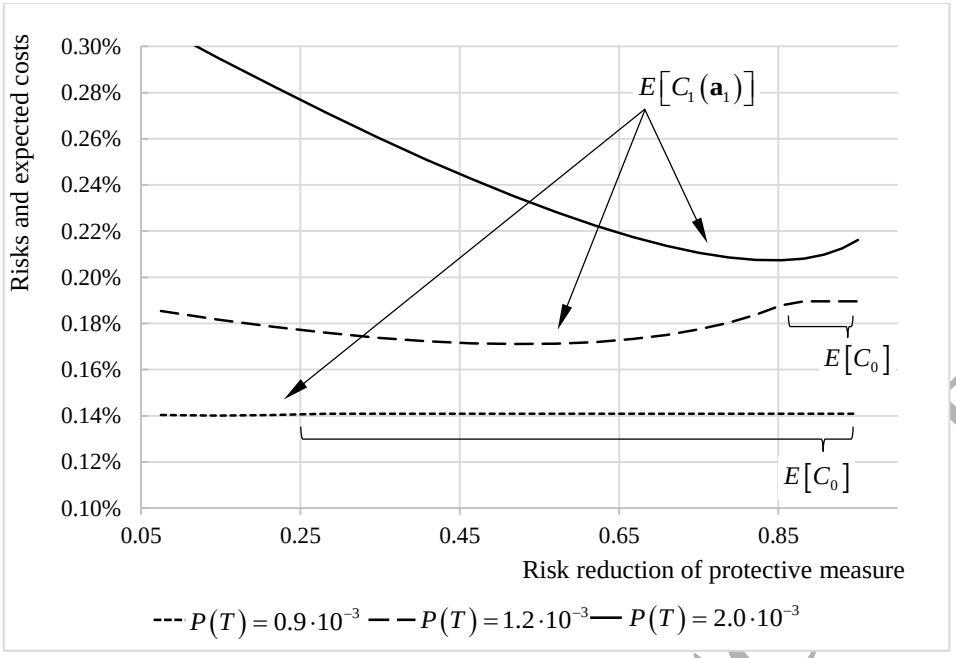

Figure 5: Minimum risks and expected costs in dependency of the protection risk reduction for different threat levels

The probability that the protection measure is cost efficient, i.e. $P\left(C_{1,i}(\ldots) > C_0\right)$, is calculated to account for the uncertainties in the models as the optimization and decision is solely based on the expectation. The cost efficiency probability increases with increasing threat probabilities, however, the probability decreases for an increasing risk reduction (Figure 6) and costs of the protective measure. It is independent of the minimum risk and expected cost in Figure 5.

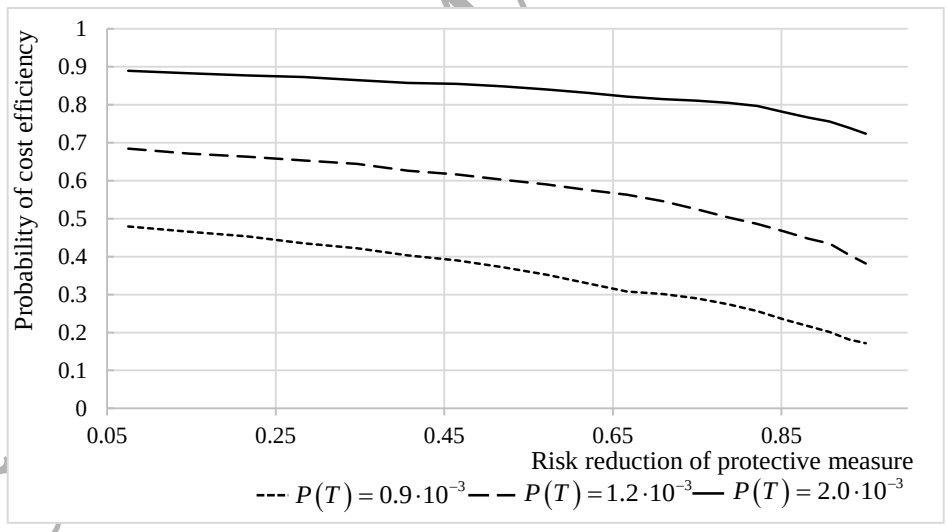

Figure 6: Probability that the protection measure is cost efficient in dependency of the protection risk reduction for different threat levels

The optimal risk mitigation strategies are identified as the minima in Figure 5 and listed in Table 4
. Only for a high threat level, a high level of the protection is optimal despite the over-proportional higher costs. It is noted that the cost efficiency probability of the protection significantly increases with the threat probability.

Table 4: Optimal protection strategies for different threat levels together with the probability of cost efficiency

Annual threat probability	Risk reduction	Annual protection costs	Probability of cost efficiency
$0.9 \cdot 10^{-3}$	0.15	0.018%	0.47
$1.2 \cdot 10^{-3}$	0.52	0.079%	0.60
$2.0 \cdot 10^{-3}$	0.85	0.161%	0.78

4.2 *Analysis of surveillance information and bridge closure actions*

The analysis and optimization of the control strategy is performed in dependency of the performance and the cost of the surveillance strategy (see Figure 3) and the aforementioned three threat levels. Figure 7 shows a change of inclination in the curve for the threat probability $0.9 \cdot 10^{-3}$. Here, the optimal action for a threat indication changes from do-nothing to closure of the bridge. The minimum risks and expected costs are located at relatively high threat indication reliabilities and associated costs.

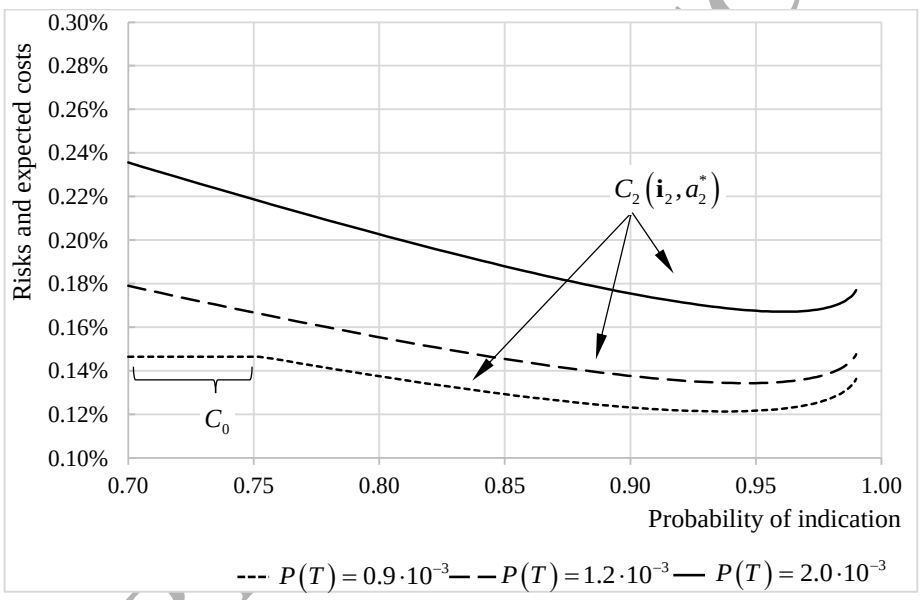

Figure 7: Minimum risks and expected costs in dependency of the surveillance performance for different threat levels

The probabilities that the surveillance and bridge closure strategy are cost efficient, $P\left(C_{2,i}\left(\ldots\right) > C_0\right)$, increase with an increasing threat indication probability (and corresponding surveillance strategy costs) until the minimum of the risks and expected costs are reached (Figure 8). The probabilities are highest for the highest threat probability.

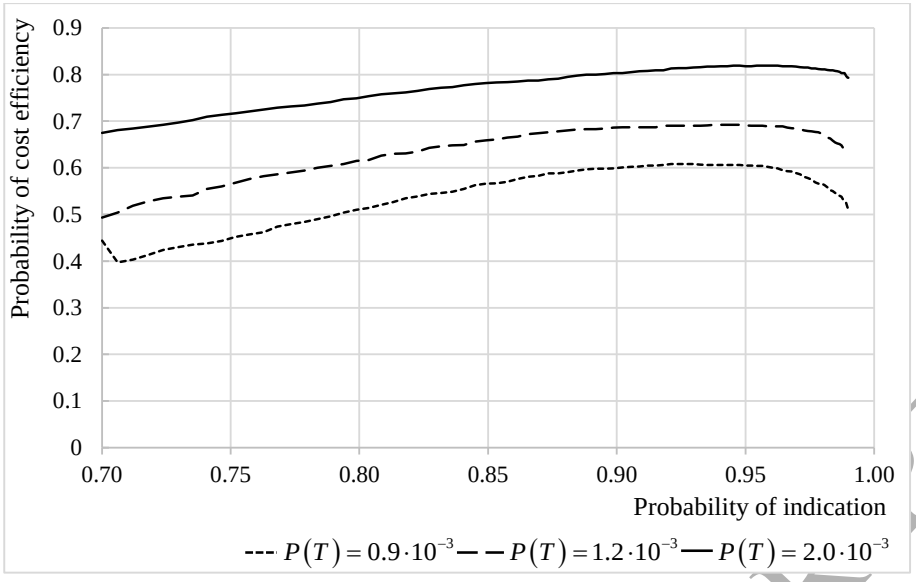

Figure 8: Probability that surveillance is cost efficient in dependency of the surveillance performance for different threat levels

The optimal surveillance strategies for the considered threat levels are very similar in indication probabilities (Table 5). The probability of cost efficiency increases significantly for higher threat probabilities.

Table 5: Optimal surveillance strategies for different threat levels together with the probability of cost efficiency

Annual threat probability	Probability of indication	Surveillance costs	Probability of cost efficiency
$0.9 \cdot 10^{-3}$	0.94	0.065%	0.61
$1.2 \cdot 10^{-3}$	0.95	0.068%	0.69
$2.0 \cdot 10^{-3}$	0.96	0.075%	0.82

Table 6 contains the identification of the optimal strategies for risk mitigation based on the minimum risks and expected costs together with the measures of significance and cost efficiency. The optimal risk mitigation strategies lead to a significant risk and excepted cost reduction of about 10% and higher with the exception of protection for a threat probability of $0.9 \cdot 10^{-3}$. It is observed that the optimal control strategies lead to higher significances. For both the strategies a very significant risk and expected cost reduction of 35.2% (Protect) and 47.8% (Control) can be achieved for an annual threat probability of $2.0 \cdot 10^{-3}$ per bridge per year. The probability of cost efficiency is higher for the control strategy, however, the difference in the probabilities decreases for a high threat level (see Table 4 and Table 5).

Table 6: Optimal protection and control strategies in comparison: performance, annual costs, significance and cost efficiency. The overall optimal strategies are bold.

Annual threat probability	Protect: s_1				Control: s_2			
	Risk reduction	Annual costs	Significance	Probability of cost efficiency	Probability of indication	Annual costs	Significance	Probability of cost efficiency
$0.9 \cdot 10^{-3}$	0.15	0.018%	<1.0%	0.47	**0.94**	**0.065%**	**13.3%**	**0.61**
$1.2 \cdot 10^{-3}$	0.52	0.079%	9.9%	0.60	**0.95**	**0.068%**	**29.3%**	**0.69**
$2.0 \cdot 10^{-3}$	0.85	0.161%	35.2%	0.78	**0.96**	**0.075%**	**47.8%**	**0.82**

5 DISCUSSION

The efficiency of risk mitigation measures is largely dependent and the analysis is highly sensitive to the threat probabilities. Any decision should thus be based on knowledge of the threat probabilities and current threat information accounting for the non-stationarity of the underlying human behavior processes. However, no mitigation strategy is expected to be cost efficient when the historical statistics are considered, which lead to an annual threat probability of $1.0 \cdot 10^{-5}$ per bridge or lower (see Section 3.1).

Beyond the specifics of the decision analysis and taking into account the potential variation of the threat levels throughout the long service life of a bridge, it should be noted that the cost efficiency of surveillance can be influenced by pausing operation for periods with low threat probabilities as this contributes largely to the annual costs. Hence, changing threats point to flexible and surveillance based systems. However, co-benefits for protective measures may be found e.g. in a higher earthquake resistance (see e.g. [3]).

A combination of protection and control strategies constitutes an attractive option for very high threat probabilities. However, for the analyzed threat probabilities, a combination will not be more significant, as the risk reduction by the protective measure will result in lower absolute values not being able to accommodate for the expected cost of the protection strategy.

6 SUMMARY AND CONCLUSIONS

This paper contains a cost efficiency assessment of risk mitigation measures for terrorist attacks with Improvised Explosive Devices (IEDs) for a large span and iconic bridge structure. The assessment is performed within a decision theoretical framework building upon very recent advances in the COST Action TU1402 on Quantifying the Value of Structural Heath Monitoring.

The decision scenario is formulated based on an authority responsible for the societal safety of the infrastructure and consequently the direct risks for the infrastructure owner and the indirect risk due to fatalities and importance of the infrastructure are considered. The risk mitigation strategies are classified within the decision theoretical context as protection measures, which may be implemented in the design phase of a structure, and as control, i.e. information acquirement, strategies. Whereas the protection measures can be analyzed with a prior decision analysis, the analysis of additional information requires a pre-posterior decision analysis and an appropriate modelling of the information before its acquirement.

The identification of efficient measures for risk mitigation is based on

1) The risk and expected cost based optimization of actions and information and their combination before implementation,
2) On quantifying and assuring significance in risk reduction and
3) On quantifying and ensuring a high probability of cost efficiency.

These criteria, i.e. the optimality, significance and efficiency ensure the performance of the strategies at the decision point in time before implementation.

Specifically, it has been found in the analysis of protective measures:

- High performance and expensive protection measures are optimal and significant for higher threat levels (larger than $2.0 \cdot 10^{-3}$ per bridge per year). The probability of cost efficiency is higher than 0.78.
- For lower threat levels between $1.2 \cdot 10^{-3}$ and $2.0 \cdot 10^{-3}$, protective measures even with a limited performance and relatively low costs may be implemented as they are optimal, however, with a limited significance of 10% to 35%.

- Below a threat level of $0.9 \cdot 10^{-3}$, protective measures are identified as optimal. However, they should not be implemented as the probability of their cost efficiency is lower than 47% and the risk and expected cost reduction is insignificant.

In contrast to the optimal protection strategies, the identified optimal control strategies have a high indication reliability and relatively high costs. The optimal control strategies are relatively insensitive to the considered threat probabilities and may thus be identified very clearly.

- The optimal control strategies should have a threat indication reliability higher than 94% with annual costs equal to 0.065% (or higher for higher indication reliabilities) per year per bridge.
- The identified optimal control strategies have a better performance than the protective strategies in terms of minimum risks, significance and cost efficiency.
- Below a threat level of $0.9 \cdot 10^{-3}$ control strategies should be carefully assessed for their significance and probability of cost efficiency.

It is acknowledged that the risk analysis and optimal setting of risk reduction measures excluded a resilience performance assessment. It is noted that the (1) integration of the Bayesian decision and utility analysis and resilience analysis and (2) the resilience analysis of infrastructure constitutes topics of very recent and future research, see e.g. [42],[43], [23] and [44].

Bayesian decision and utility analyses in general and in conjunction with their complexity and computational demands should contain or provide interfaces (as with this paper) to (1) sophisticated models such as e.g. for the structural performance modelling for explosive loadings, (2) non-public (e.g. threat) information and (3) sophisticated information acquirement performance models. In return, these models and information should be available in the format, quality, and relevance required by the decision analysis to ensure transparent, consistent and sustained decisions. For further research and evolution of decision analyses, interface design, model development and availability are seen as the most challenging aspects, however, with a clear and substantial potential to benefit society.

ACKNOWLEDGEMENTS

The COST Action TU1402 on Quantifying the Value of Structural Health Monitoring (www.cost-tu1402.eu) is gratefully acknowledged for the inspiring discussions, contributions and workshops across the scientific and engineering disciplines with researchers, industrial experts and representatives of infrastructure operators, owners and authorities.

The visiting fellowship provided by the Centre for Infrastructure Performance and Reliability at The University of Newcastle for the first author is gratefully acknowledged.

7 REFERENCES

[1] Stewart MG, Mueller J. Terrorism Risks for Bridges in a Multi-Hazard Environment. International Journal of Protective Structures. 2014;5:275-89.
[2] Ellingwood BR. Mitigating Risk from Abnormal Loads and Progressive Collapse. Journal of Performance of Constructed Facilities. 2006;20:315-23.
[3] Stewart MG. Risk of Progressive Collapse of Buildings from Terrorist Attacks: Are the Benefits of Protection Worth the Cost? Journal of Performance of Constructed Facilities. 2017;31:04016093.

[4] Xiao W, Andrae M, Ruediger L, Gebbeken N. Numerical prediction of blast wall effectiveness for structural protection against air blast. Procedia Engineering. 2017;199:2519-24.
[5] Mueller JE, Stewart MG. Chasing Ghosts - The Policing of Terrorism. New York, USA: Oxford University Press; 2016.
[6] SeRoN Consortium. Security of Road Networks: Final Report. 2012.
[7] Joshi NN, Lambert JH. Diversification of infrastructure projects for emergent and unknown non-systematic risks. Journal of Risk Research. 2011;14:717-33.
[8] Thorisson H, Lambert JH. Multiscale identification of emergent and future conditions along corridors of transportation networks. Reliability Engineering and System Safety. 2017;167:255-63.
[9] Leung M, Lambert JH, Mosenthal A. A risk-based approach to setting priorities in protecting bridges against terrorist attacks. Risk Analysis. 2004;24:963-84.
[10] Thekdi SA, Lambert JH. Integrated risk management of safety and development on transportation corridors. Reliability Engineering & System Safety. 2015;138:1-12.
[11] Bedon C, Zhang X, Santos F, Honfi D, Kozłowski M, Arrigoni M, et al. Performance of structural glass facades under extreme loads – Design methods, existing research, current issues and trends. Construction and Building Materials. 2018;163:921-37.
[12] Mouritz AP, Rajapakse YDS. Explosion Blast Response of Composites. Woodhead Publishing; 2017.
[13] Netherton MD, Stewart MG. Blast Load Variability and Accuracy of Blast Load Prediction Models. International Journal of Protective Structures. 2010;1:543-70.
[14] Grant MJ, Stewart MG. Modelling improvised explosive device attacks in the West – Assessing the hazard. Reliability Engineering & System Safety. 2017;165:345-54.
[15] Stewart MG. Reliability-based load factor design model for explosive blast loading. Structural Safety. 2018;71:13-23.
[16] Hausken K, He F. On the Effectiveness of Security Countermeasures for Critical Infrastructures. Risk Analysis. 2016;36:711-26.
[17] Von Neumann, Morgenstern. Theory of Games and Economical Behavior. 2nd Edition ed: Princeton University Press, Princeton.; 1947.
[18] Raiffa H, Schlaifer R. Applied statistical decision theory. Wiley classics library, Originally published: Boston : Division of Research, Graduate School of Business Administration, Harvard University, 1961. ed. New York: Wiley (2000); 1961.
[19] Pfanzagl J. Subjective probability derived from the morgenstern-von neumann utility concept. Princeton University Press; 2015. p. 237-51.
[20] Brocklehurst S. Everything you need to know about the Queensferry Crossing. BBC Scotland, 27 August 2017; 2017.
[21] Halstead R. Building the Golden Gate Bridge today would be no easy task. The Mercury News, 27 May 2002; 2002.
[22] Thöns S. On the Value of Monitoring Information for the Structural Integrity and Risk Management. Computer-Aided Civil and Infrastructure Engineering. 2018;33:79-94.
[23] Faber MH, Qin J, Miraglia S, Thöns S. On the Probabilistic Characterization of Robustness and Resilience. Procedia Engineering. 2017;198:1070-83.
[24] SeRoN Consortium. Security of Road Networks: Risk Assessment. 2012.
[25] Blue Ribbon Panel on Bridge and Tunnel Security. Recommendations for Bridge and Tunnel Security, US Federal Highway Administration (FHWA). 2003.
[26] Mueller J, (ed.). Terrorism Since 9/11: The American Cases. http://politicalscience.osu.edu/faculty/jmueller/since.html. 2018.
[27] Grant M, Stewart MG. A systems model for probabilistic risk assessment of improvised explosive device attacks. International Journal of Intelligent Defence Support Systems. 2012;5:75-93.
[28] Das R, Pandey AD, Soumya, Mahesh MJ, Saini P, Anvesh S. Progressive Collapse of a Cable Stayed Bridge. Procedia Engineering. 2016;144:132-9.
[29] Mozos CM, Aparicio AC. Parametric study on the dynamic response of cable stayed bridges to the sudden failure of a stay, Part I: Bending moment acting on the deck. Engineering Structures. 2010;32:3288-300.
[30] Lonetti P, Pascuzzo A. Vulnerability and failure analysis of hybrid cable-stayed suspension bridges subjected to damage mechanisms. Engineering Failure Analysis. 2014;45:470-95.

[31] Mueller J, Stewart MG. Terror, Security and Money: Balancing the Risks, Benefits, and Costs of Homeland Security: Oxford University Press, USA; 2011.
[32] Robinson Lisa A, Hammitt James K, Aldy Joseph E, Krupnick A, Baxter J. Valuing the Risk of Death from Terrorist Attacks. Journal of Homeland Security and Emergency Management2010.
[33] SeRoN Consortium. Security of Road Networks: Validation. 2012.
[34] Bram J, Orr J, Rapaport C. Measuring The Effects of the September 11 Attack on New York City. FRB-NY Economic Policy Review. 2002.
[35] Blomberg S, Rose A. Editor's Introduction to the Economic Impacts of the September 11, 2001, Terrorist Attacks. Peace Economics, Peace Science, and Public Policy. 2009;15:1-16.
[36] Cheng HY, Weng CC, Chen YY. Vehicle Detection in Aerial Surveillance Using Dynamic Bayesian Networks. IEEE Transactions on Image Processing. 2012;21:2152-9.
[37] Benfold B, Reid I. Stable multi-target tracking in real-time surveillance video. CVPR 20112011. p. 3457-64.
[38] Jiang F, Wu Y, K. Katsaggelos A. Abnormal event detection from surveillance video by dynamic hierarchical clustering. 2013.
[39] Davies ER. Computer Vision: Principles, Algorithms, Applications, Learning: Elsevier; 2018.
[40] Tsakanikas V, Dagiuklas T. Video surveillance systems-current status and future trends. Computers & Electrical Engineering. 2017.
[41] Xu N, Chen CH, Hauswald S, Evers C. Influence factors of probability of detection test on surveillance systems. 2011 Integrated Communications, Navigation, and Surveillance Conference Proceedings2011. p. N3-1-N3-8.
[42] Miraglia S, Faber MH, Thöns S, Stewart M. Resilience of systems by value of information and SHM. ICOSSAR 2017. Vienna, Austria2017.
[43] He X, Cha EJ. Modeling the damage and recovery of interdependent critical infrastructure systems from natural hazards. Reliability Engineering & System Safety. 2018;177:162-75.
[44] Bostick TP, Connelly EB, Lambert JH, Linkov I. Resilience science, policy and investment for civil infrastructure. Reliability Engineering & System Safety. 2018;175:19-23.