

# Complex-system decision framework for managing risks to rail stations at airports from terrorist threats

Alawad, Hamad Ali H; Codru, Silviu; Kaewunruen, Sakdirat

DOI:

[10.5592/CO/CETRA.2018.665](https://doi.org/10.5592/CO/CETRA.2018.665)

License:

Creative Commons: Attribution (CC BY)

*Document Version*

Publisher's PDF, also known as Version of record

*Citation for published version (Harvard):*

Alawad, HAH, Codru, S & Kaewunruen, S 2018, Complex-system decision framework for managing risks to rail stations at airports from terrorist threats. in *The 5th International Conference on Road and Rail Infrastructure*. University of Zagreb, pp. 885-861, The 5th International Conference on Road and Rail Infrastructure , Zadar, Croatia, 17/05/18. <https://doi.org/10.5592/CO/CETRA.2018.665>

[Link to publication on Research at Birmingham portal](#)

## **Publisher Rights Statement:**

Checked for eligibility: 24/05/2018

"Authors retain copyright over their work, while allowing the conference to place this unpublished work under a Creative Commons Attribution License, which allows others to freely access, use, and share the work, with an acknowledgement of the work's authorship and its initial presentation at this conference."

## **General rights**

Unless a licence is specified above, all rights (including copyright and moral rights) in this document are retained by the authors and/or the copyright holders. The express permission of the copyright holder must be obtained for any use of this material other than for purposes permitted by law.

- Users may freely distribute the URL that is used to identify this publication.
- Users may download and/or print one copy of the publication from the University of Birmingham research portal for the purpose of private study or non-commercial research.
- User may use extracts from the document in line with the concept of 'fair dealing' under the Copyright, Designs and Patents Act 1988 (?)
- Users may not further distribute the material nor use it for the purposes of commercial gain.

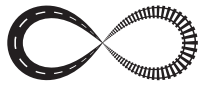
Where a licence is displayed above, please note the terms and conditions of the licence govern your use of this document.

When citing, please reference the published version.

## **Take down policy**

While the University of Birmingham exercises care and attention in making items available there are rare occasions when an item has been uploaded in error or has been deemed to be commercially or otherwise sensitive.

If you believe that this is the case for this document, please contact [UBIRA@lists.bham.ac.uk](mailto:UBIRA@lists.bham.ac.uk) providing details and we will remove access to the work immediately and investigate.



## COMPLEX-SYSTEM DECISION FRAMEWORK FOR MANAGING RISKS TO RAIL STATIONS AT AIRPORTS FROM TERRORIST THREATS

Hamad Alawad<sup>1,2</sup>, Silviu Codru Second<sup>1</sup>, Sakdirat Kaewunruen<sup>1,2</sup>

<sup>1</sup> The University of Birmingham, School of Engineering, Department of Civil Engineering, TOFU Lab (Track Engineering and Operations for Future Uncertainties), United Kingdom

<sup>2</sup> The University of Birmingham, Birmingham Centre for Railway Research and Education, United Kingdom

### Abstract

This paper describes a risk-based decision-making framework aimed at helping stakeholders of transport infrastructure to allocate (limited) resources effectively, in order to mitigate the risk of a terrorist attack. The framework is used to model the security system, to consider a multitude of threat scenarios and to assess the decisions taken by the aggressors during the various stages of their attack. One of the key notions presented is the state of partial neutralization, which reveals the losses that incur when the terrorist does not reach the primary target. A rail station of an airport is used as an example to demonstrate this framework.

*Keywords: decision analysis, infrastructure security, probabilistic risk assessment, terrorism*

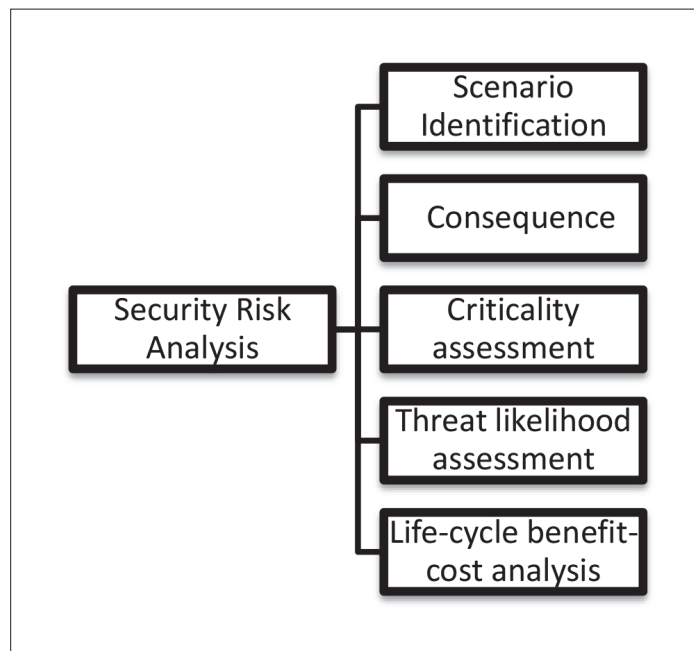
### 1 Introduction

Civil The terrorist attacks of September 11th, 2001 in the United States, inflicted heavy economic losses and, numerous casualties, and the unprecedented effects that followed these attacks have prompted policy makers and the public to make considerable efforts towards the development of tools and approaches that estimate the risk of terrorism and aid with the implementation of security policies to reduce this risk. Furthermore, many potential attack scenarios have been proposed, and a large number of responses have been employed or advised [1]. A better comprehension of the actions of terrorists and the way they select certain targets of attack can aid in making the decisions and helping the security designers to allocate resources in the fight against terrorism [2]. To face the challenge of terrorism, new analytical methods and new institutional arrangements must be elaborate, as per Making the Nation Safer, a report by the National Research Council [3]. Infrastructure is not an independent system but rather is linked with other interdependent systems. A failure of the electrical power grid, for example, may affect not only the energy sector but also in a cascading effect may result in the collapse or severe disruption of transportation, telecommunications, public health, and banking and financial systems of the country [4]. As the infrastructure is typically complex, and many issues can arise during the decision-making process, a risk management framework is required to acknowledge all the parameters and uncertainties involved. Modelling risk and decision frameworks is appropriate for risk managers to derive the most suitable risk management measures [5]. Decision analysis as a subset of decision notions has been known of since 1963 (Howard and Matheson, 1989). Decision analysis recognises the three main features associated with all decisions: risks, benefits, and costs. [4] showed the cost-benefit analytical method has a wide range of applications (economics, finance,

probability, reliability etc.) The effect of all these fields on decision boost is well defined in the literature e.g., [6-8]. Many methods have been devised in an attempt to model and assess the efficiency of counter-terrorism procedures. Some of these methods involve game-theoretic approaches which are used to model how intelligent attackers and defenders interact. Another set of methods is based on probabilistic risk assessment or PRA. PRA has been used to evaluate the risks associated with complex engineered entities and it recently started being used to assess terrorism risk. Moreover, PRA aids analysis and decision-maker to understand and describe the risks which is predict the probable consequences [9]. We presented [10] the framework for Managing Risk to deal with the risk analysis of situations where considering the state of partial neutralization of an attacker means the likely loss incurred in two scenarios can be estimated. In the first scenario the attacker would be successful in the attack on the primary target while in the second one, in spite of failing to reach his primary target, they would still cause significant damage to the infrastructure, threaten human life and affect the financial market. By breaking down a security system into individual layers, each with their own probabilities of an attacker being detected, engaged and neutralized an accurate model can be obtained. In addition, it is also assumed that the terrorists are rational and would try to maximize their chances of succeeding with the attack. In this paper, the security improvement of an airport rail station will be used to illustrate the effectiveness of the proposed and then deals with cost assessment for mitigating the total risk and cost-effectiveness of the measures as a futur work.

## 2 Security risk analysis

The proposed framework breaks down the risk analysis into five main process components as shown in Fig. 1 below, where a separation of these main components reveals the key risk providers and the critical parameters that add to the uncertainty and form a framework for critical asset and processes for risk analysis [11-15]



**Figure 1** Five main components of Security Risk Analysis

## 2.1 Scenario identification

During this first step of the risk analysis the possible threat scenarios are determined. Worldwide since the 1990s, transportations systems have been targeted by terrorist attacks and this form of terrorist threats encompasses a wide range of potential attacks and more likely scenarios Fig. 2 [16].

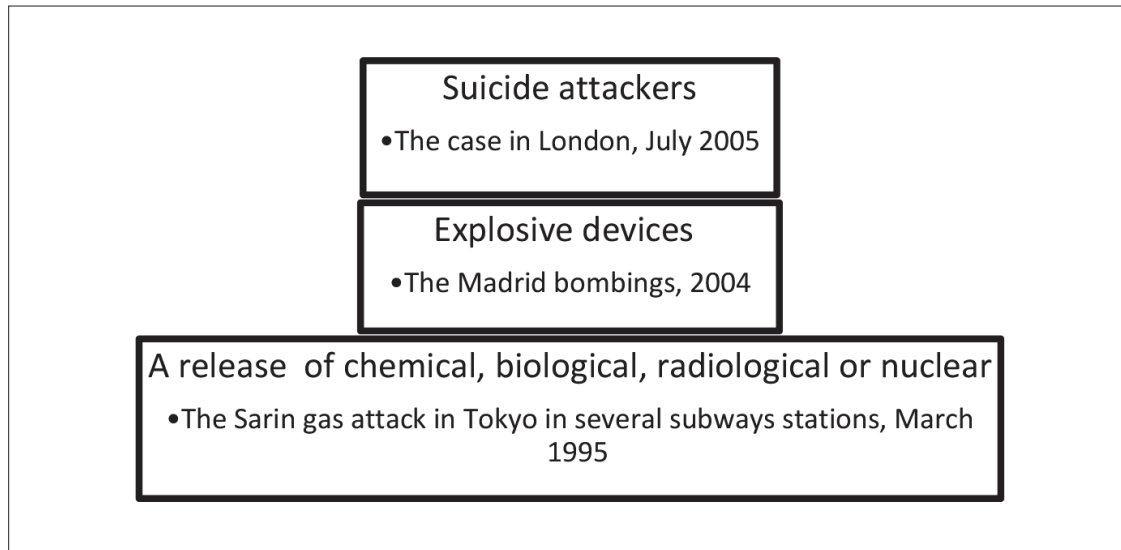


Figure 2 The forms of terrorist threats in the public transportations

## 2.2 Consequence and criticality assessment

this assessment provides the estimated losses of a successful attack. In the area of counter-terrorism the term loss has various meanings, such as damage to the environment, human casualties, impact on society, as well as economic losses either direct or indirect due to physical damage, interruptions of business and financial market insecurity. These different types of losses can be estimated using game-theoretic methods and modeling means such as event trees, fault trees and decision trees. In order to assess the efficiency of the various countermeasures, all these losses are converted to a single value which reflects the financial loss by pricing casualties with insurance data.

## 2.3 Security vulnerability assessment

to understand and measure the impact of threats such as terrorism, the risk analysis and evaluation of threats and vulnerabilities are significant methods and thus the output is very valuable information for decision makers to select the optimal countermeasures to manage threats. The third step of this risk analysis reveals the probability that a terrorist is successful in attacking their target with the condition that they initiated the attack. By combining this probability with the estimates of possible losses of key assets conditioned on the success of the attack, the main conditional expected loss associated with a scenario is revealed. The successful attack is based on the terrorist's ability to defeat the security system. The defensive system comprises of a number of sequential steps: detection of the attacker, engagement upon detection and neutralization upon engagement (see Fig. 3). Each security zone is represented by specific components used for detection, engagement and neutralization. Therefore, in security zone  $i$  the probability that the defenders engage the attacker upon detection would be  $P_{Di}$ , the probability that the defenders engage the attacker in security zone  $i$  upon detection

in security zone  $j$  is represented by  $P_{Ei|Dj}$ , and the probability that the attacker is neutralized in security zone  $i$ , after engagement in security zone  $j$ , is expressed by  $P_{Ni|Dj}$ .

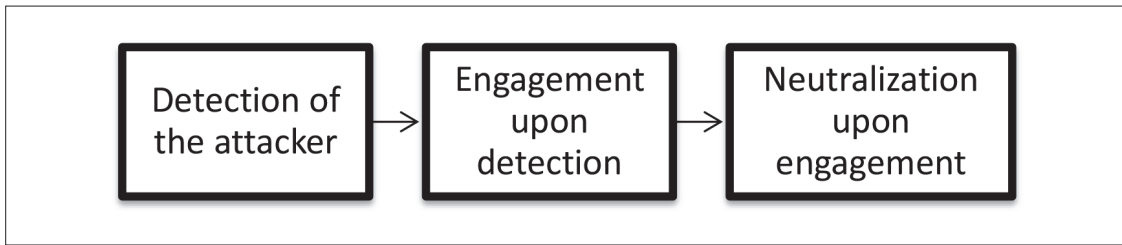


Figure 3 The defensive system process

The losses from an unsuccessful attack can be estimated by defining two states of neutralization. In the first state the attacker is completely neutralized and is not able to inflict any damage to his surroundings. This state is labeled as neutralization of type 1 or full neutralization and is denoted by  $N_{i,1}$  for the security zone  $i$  with a probability of  $P_{Ni,1}$ . The second state of partial neutralization is used for the situations in which the terrorist is denied access to the following security zone but is not completely neutralized and therefore is still able to cause damage to the surroundings. The state of partial neutralization is labeled as type 2, denoted by  $N_{i,2}$ , with a probability of  $P_{Ni,2}$ . However, the defenders fail to neutralize the attacker, then the attacker can proceed to the next security zone. In this situation the probability is equal to  $1 - (P_{Ni,1} + P_{Ni,2})$ .

Taking into account that all the means of detection are interconnected in all security zones, the attacker would only need to be detected in one security zone for full detection across all security zones. It is then safe to assume that either the engagement or the neutralization of the attacker failed in zone  $i$  if they are able to pass to the next security zone  $i+1$  where they will be subsequently engaged. The probability associated with this situation would be  $P_{Ei+1|Di}$  and an illustration is provided in Fig. 4 & Table 1, for a hypothetical asset with two security zones in series.

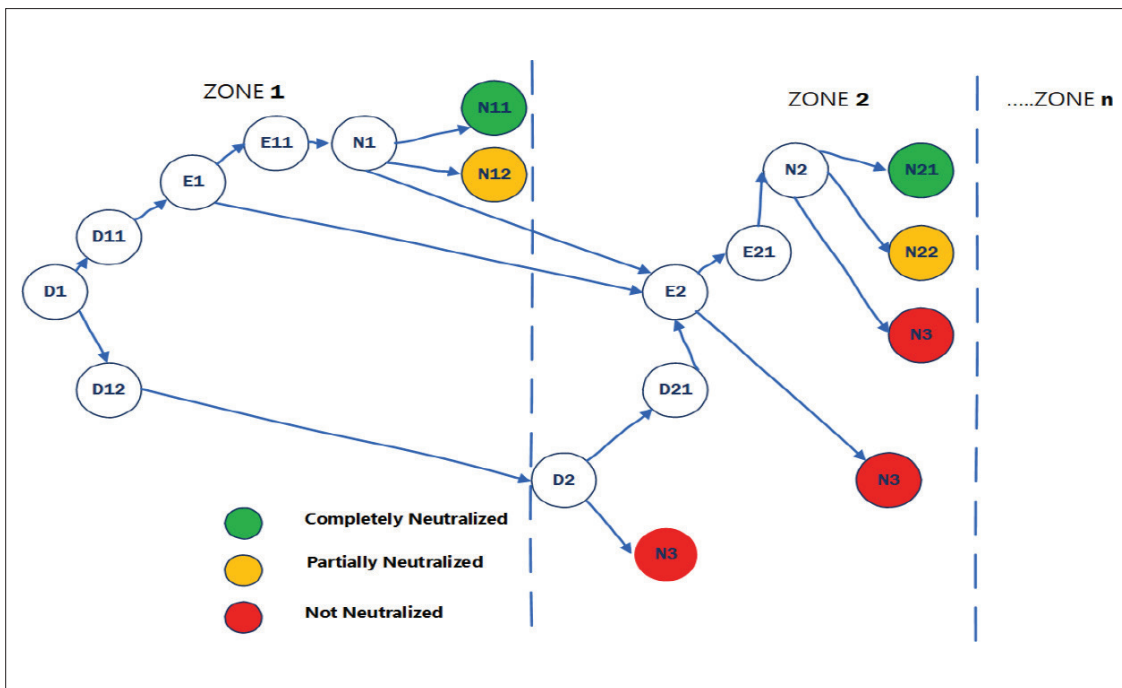


Figure 4 Hypothetical asset with two security zones

**Table 1** The Assumed defensive system process symbols.

The events Scenario		Zone1	Zone2
<b>Detection</b> (D1, D2)	Detected	D11	D21
	NOT	D12	---
<b>Engagement</b> (E1, E2)	Engaged	E11	E21
	NOT	---	---
<b>Neutralization</b> (N1, N2)	Completely	N11	N21
	Partially	N12	N22
	NOT	---	N 3

Therefore, the probability that the attacker is completely neutralized, i.e., interdiction of type 1 (m=1), or partially neutralized, i.e., interdiction of type 2 (m=2), is shown in Eq. (1).

$$P_{ES,m} = P_{D1} \left\{ P_{E1|D1} P_{N1,m|E1} + \sum_{i=2}^n P_{Ei|D1} P_{Ni,m|Ei} * \prod_{j=1}^{i-1} [(1 - P_{Ej|D1}) + P_{Ej|D1} (1 - P_{Ni,1|Ej} - P_{Ni,2|Ej})] \right\} + \quad (1)$$

$$\sum_{k=2}^n P_{Dk} \left\{ \prod_{l=1}^{k-1} (1 - P_{Dl}) \right\} \left\{ P_{Ek|Dk} P_{Nk,m|Ek} + \sum_{i=k+1}^n P_{Ei|Dk} P_{Ni,m|Ei} \prod_{j=k}^{i-1} [(1 - P_{Ej|Dk}) + P_{Ej|Dk} (1 - P_{Ni,1|Ej} - P_{Ni,2|Ej})] \right\}$$

The probability of a successful attack is achieved by:

$$P_s = P_{\bar{ES}} P_{KSA} \quad (2)$$

Where  $P_{\bar{ES}} = (1 - P_{ES,1} - P_{ES,2})$  is the probability that the defenders fail to stop the attacker and  $P_{KSA}$  is the probability conditioned by a successful attack providing that the defenders fail to stop the attacker [10].

## 2.4 Treat likelihood assessment

one of the main steps in security risk analysis is creating a model of the decision making process during which the attackers pick their best options and alternatives to execute the attack. Utility theory can be used to factor risk aversion into the decision process, and this section will infer utility functions that represent attacker profiles in threat Likelihood Assessment [17-20]. Their preferences can be illustrated by utility functions that order the alternative choices of the attackers by preference in a certain stage of the attack. [1] Terrorists maximize the expected utility by choosing the appropriate attack profile, threat scenario and asset to attack. The attacker's utility function focuses on the maximum loss brought to the defenders, reducing their loss in the case of an unsuccessful attack and minimizing the cost of execution.

## 2.5 Life-cycle cost assessment

for the decision maker, it is essential to have analytical tools comparing and assessing risk against the costs. If the loss feature is in units other than cost (such as fatalities) and for assessing the costs and benefits of counter-terrorism (CT), which denote protective measures for infrastructure, it is concluded that to define cost-effectiveness the incremental cost-effectiveness ratio (CER) is used, as explained [8]:

$$\frac{\text{cost spent on CT measure}}{\text{losses avoid by CT measure}} \quad (3)$$

### 3 Conclusion

Security risk assessment aims to identify the most efficient risk reduction options while taking into account a limited budget. Generally, these options include the reduction of the probability of attacks and the potential losses following an attack. The efficiency is obtained by observing the reduction in total loss upon the application of the mitigation method while taking into account the cost of implementation. It is clear that a terrorist attack on one part of the infrastructure such as railway stations in the airports could cause a serious loss of lives and deterioration of the economy and infrastructure as a whole. Thus, management of risk to vital infrastructure is crucial for prosperity in our modern society. Terrorist attacks have been determined as a major source of risk and stakeholders and decision makers have made considerable efforts to develop tools that aid with risk mitigation. The difference between a natural risk and a terrorism risk is that the latter is planned by an intelligent aggressor and therefore it cannot be modeled using a random approach. To manage this risk, one must consider the human behaviour in identifying possible terrorist threats and their consequences. This paper presents a risk assessment of the framework presented by Shafieezadeh, etc [10], which can be used to alleviate the risk of terrorist attacks on transport infrastructure, and it highlights the possibility of partial neutralization of the attacker.

### References

- [1] Paté-Cornell, E., Guikema, S.: "Probabilistic modeling of terrorist threats: A systems analysis approach to setting priorities among countermeasures.," *Military Operations Research*, vol. 7, no. 4, pp. 5-23, 2002.
- [2] Keeney, L.G., von Winterfeldt, D.: "Identifying and Structuring the Objectives of Terrorists," *Risk Analysis*, vol. 30, no. 12, pp. 1803-1816, 2010.
- [3] NRC, "Making the nation safer: the role of science and technology in countering terrorism," *The National Academies*, Washington, DC, 2002.
- [4] Garrick, B.J., Hall, E.J., Kilger, M., McDonald, C.J., O'Toole, T., Probst, S.P., Zebroski, E.L.: "Confronting the risk of terrorism :Making the right decision," *Reliability Engineering & System Safety*, vol. 86, no. 2, p. 129–176, 2004.
- [5] Terje, A., Ortwin, R.: "The Role of Quantitative Risk Assessments for Characterizing Risk and Uncertainty and Delineating Appropriate Risk Management Options, with Special Emphasis on Terrorism Risk," *Society for Risk Analysis*, vol. 29, no. 4, 2009.
- [6] Jordaan, I.: *Decisions Under Uncertainty: Probabilistic Analysis for Engineering Decisions*, Cambridge: Cambridge University Press, 2005.
- [7] Bammer, G., Smithson, M.: *Uncertainty and Risk: Multidisciplinary Perspectives*, London: Earthscan Publications, 2008.
- [8] Stewart, G.M.: "Risk-informed decision support for assessing the costs and benefits of counter-terrorism protective measures for infrastructure," *International Journal of Infrastructure Protection*, p. 29 – 40, 2010.
- [9] Bier, V.M.: "Probabilistic risk analysis," in *Risk in Extreme Environments: Preparing, Avoiding, Mitigating, and Managing*, Routledge, 2017, p. 192.
- [10] Shafieezadeh, A., Cha, E.J., Ellingwood, B.R.: "A Decision Framework for Managing Risk to Airports from Terrorist Attack," *Risk Analysis*, vol. 35, no. 2, pp. 292-306, 2015.
- [11] Ayyub, B.M., McGill, W.L., Kaminskiy, M.: "Critical Asset and Portfolio Risk Analysis: An All- Hazards Framework," *Risk Analysis*, vol. 27, no. 4, pp. 790-800, 2007.
- [12] Kaewunruen, S., Sussman, J.M., Matsumoto, A.: *Grand Challenges in Transportation and Transit Systems*. *Front. Built Environ.* 2:4, 2016. doi: 10.3389/fbuil.2016.00004

- [13] Kaewunruen, S.: Underpinning systems thinking in railway engineering education, *Australasian Journal of Engineering Education*, in press, 2018. doi:10.1080/22054952.2018.1440481
- [14] Lawrence, V., Kaewunruen, S., Bartoli, G., Baniotopoulos, C.: CFD simulation of passenger hazard risk at railway station platforms due to explosive air blasts, *The 4th Thailand Rail Academic Symposium (TRAS 2017)*, Khao Yai, Pakchong, Nakhon Ratchasima, Thailand, August 31 – September 1, 2017. <https://www.tras2017.com/>.
- [15] Sanchez, M.M.: “Security risk assessments in public transport networks,” *Rail and Rapid Transit*, vol. 225 Part F, 2010.
- [16] Stewart, G.M., Mueller, J.: Aviation Security, Risk Assessment, and Risk Aversion for Public Decisionmaking, *Policy Analysis and Management*, 32 (2013) 3, pp. 615–633.
- [17] Garcia, M.L.: “Chapter 2 – Introduction to Vulnerability Assessment,” in *Effective Physical Security*, Butterworth-Heinemann, 2017, pp. 23-53.
- [18] Lawrence, V., Ngamkhanong, C., Kaewunruen, S.: An Investigation to Optimize the Layout of Protective Blast Barriers Using Finite Element Modelling, *IOP Conference Series: Materials Science and Engineering*, 280, 2017. doi: 10.1088/1757-899X/280/1/012035
- [19] Kaewunruen, S., Pompeo, G., Bartoli, G.: Blast simulations and transient responses of long-span glass roof structures: A case of London’s railway station, *Proceedings of the 25th UKACM Conference on Computational Mechanics*, 12–13 April 2017, University of Birmingham, Birmingham, U.K. [[https://works.bepress.com/sakdirat\\_kaewunruen/83/](https://works.bepress.com/sakdirat_kaewunruen/83/)]
- [20] Sa’adin, S.L.B., Kaewunruen, S., Jaroszweski, D.: Operational readiness for climate change of Malaysia high-speed rail, *Proc. Inst. Civ. Eng. Transp* 169 (5), 308-320, 2016. doi: 10.1680/jtran.16.00031