Academic analysis of the ICE Report 'In Plain Sight: Reducing the Risk of Infrastructure Failure'

Final Report

Dr Ksenia Chmutina, Prof Alistair Gibb, Prof Andrew Dainty, Dr Lee Bosher
School of Architecture, Building and Civil Engineering, Loughborough University

Abstract

This is the final report from Loughborough University's commission from the Institution of Civil Engineers (ICE) to carry out an academic evaluation of the applicability and validity of the ICE's 12 Lines of Defence model, produced for infrastructure in response to the Grenfell Tower fire. Having reviewed the main report, the interview transcripts and associated literature we consider that this adaption of Reason's Swiss Cheese Model as a basis of the Lines of Defence is appropriate, especially as it is well recognised and understood by a wide range of stakeholders. This notwithstanding, it does have some deficiencies, and so we have proposed enhancements including an integration of post-incident analysis, appreciation for crosscutting influencers that could positively or negatively impact every line of defence, and a general risk management framework that would act as a context setting for the model and ensure that the model can be understood by non-experts, and without specific prior knowledge of the industry. The changes have been proposed in order to increase and extend the reach of the model, without compromising its recognition and effectiveness.

Introduction

The ‘In Plain Sight: Reducing the Risks of Infrastructure Failure’ interim report has been published in 2017. The aim of this document is to provide an academic evaluation of the applicability and validity of ’12 Lined of Defence’ model (Figure1).

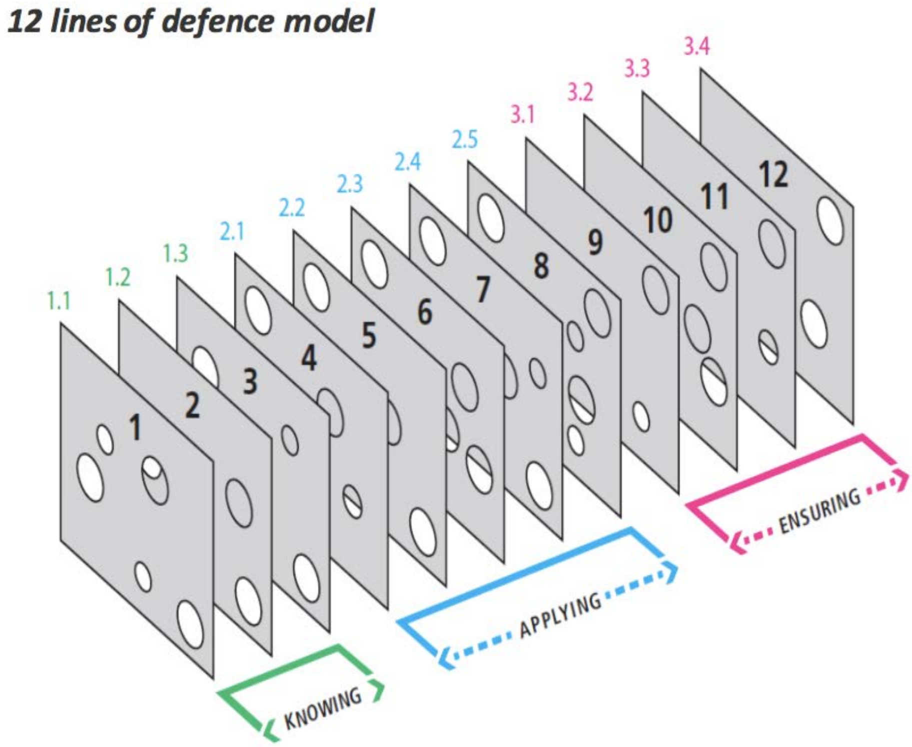


Figure 1 12 Lines of Defence Model

The task to Loughborough University comprised the following:

- In-depth analysis of the report exploring the purpose of the model and its gaps, and comparison with existing defence models;
- A random sample of interviews[1] and workshop notes as well as referenced literature to inform the model;
- An initial set of criteria allowing for academic and expert testing of the model.

The first section of this report describes the process of academic assurance; Section 2 describes the analysis of the model; and Section 3 introduces the suggested changes.

[1] *Due to the relatively small number of interviews (11), all the interview notes were reviewed.*

1. Methodology

This section describes the process of academic evaluation and provides an overview of the tasks completed during this process. The evaluation process aimed to answer the following questions:

- Why has the Swiss Cheese Model been chosen as a basis for the 12 Lines of Defence model?
- Is the model flexible enough to adjust to a changing context?
- What are the main influencers that have not been included in the model but could increase the holes in the lines of defence?
- Do layers include conflicting or crosscutting vulnerabilities?

1.1 Review of the literature and interview samples

The literature used in the report has been grouped in order to understand: what sources have been used, when the literature used was published, and what type of publication has been used. The results are presented in Figures 2a-2c.

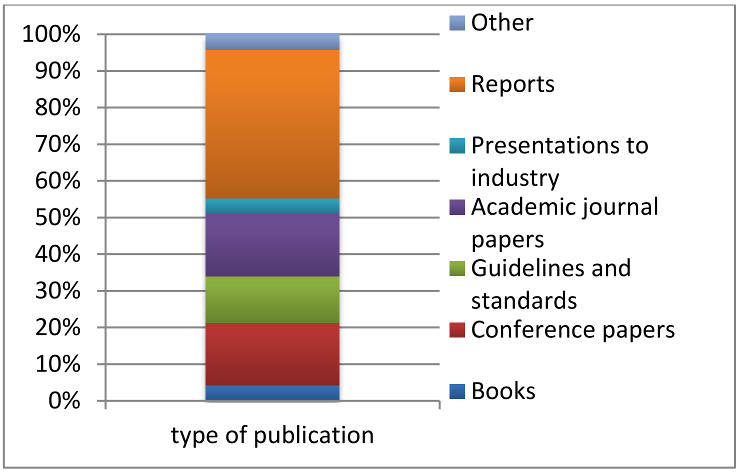


Figure 2a Types of publications (n=47)

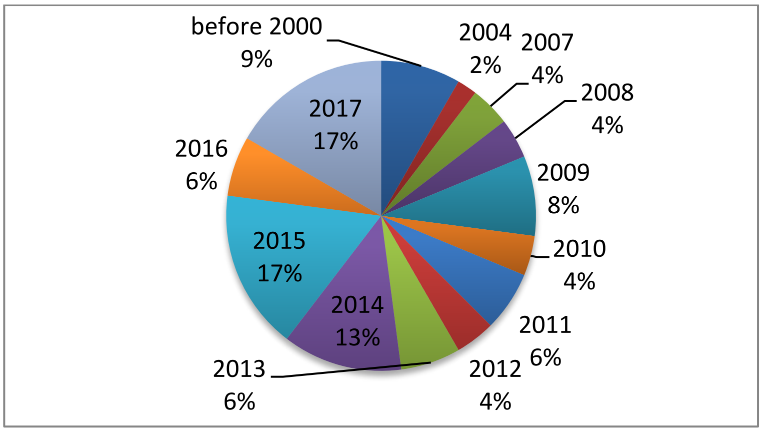


Figure 2b Source of publications

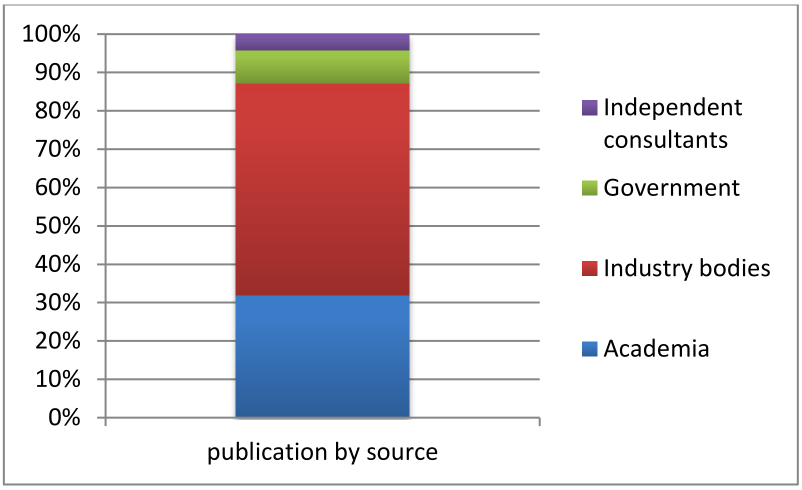


Figure 2c Date of publication

The analysis demonstrated that a breadth of literature had been used to inform the ICE report; however, literature relevant to other defence models (e.g. Bowtie model) had not been included. Other models have been reviewed as a part of the academic exercise and are described in more detail in section 2.

The content of all of the interview notes (11 in total) was also analysed, with the aim to identify how the holes in the lines of defence were informed and whether any other holes should be included. This is discussed in section 2.1.

Based on the analysis of other models and primary data, further holes were suggested and crosscutting issues identified, leading to proposing slight changes in the model as discussed in section 3.

1.2 Evaluation exercises

Two exercises have been used to test the viability of proposed changes to the model – an academic one (30th April 2018) and an expert one (23rd May). The academic exercise[2] provided an opportunity to review the suggested additional holes and develop the crosscutting influencers (Section 3.1) and recommendations.

The expert exercise aimed at testing whether the crosscutting issues suggested in the academic exercise are truly crosscutting. The ICE panel members[3] were asked to complete an exercise (Appendix A), to understand whether the model supports holistic considerations that could help prevent the failure. The experts were also asked to evaluate whether a holistic risk identification checklist (section 3.3) is appropriate to aid the understanding of the model by those who lack experience in the industry.

[2] The academic exercise was carried out among the authors of this report

[3] The participants of the expert exercise were Peter Hansford, Mike Napier and Matthew Symes

2. Analysis of the model

In recent years, a number of models that attempt to explain the causes of incidents / disasters and risk management have been developed (e.g. Petersen, 1996; Loosemore, 1998; Suraji et al. 2001; Abdelhamid and Everett, 2000). One of the most recognised and well-known models is James Reason's 'Swiss Cheese Model' (1990). To test the applicability of the Swiss Cheese Model proposed in the ICE's interim report, several other models have been reviewed from a theoretical perspective; this has led to the proposed incorporation of some of their elements into the Lines of Defence model as follows:

Bowtie model is a process for understanding the dynamics of potential major accidents. The model displays the links between the potential causes, preventative and mitigative controls and consequences of a major incident.

Integrated resilience framework is adapted from ISO 31000 aiming to engage local stakeholders (who can typically be disengaged in disaster risk reduction matters) in identifying vulnerabilities and improving urban spaces with respect to 'security threats'. Whilst the framework cannot accurately predict every threat or hazard nor provide the solution for the prevention or mitigation, it helps the various stakeholders consider prior knowledge of existing hazards and threats in a local context and to recognise that, too often, disasters occur because risk reduction measures have not been considered or undertaken (Bosher 2014; Chmutina et al., 2014).

2.1 Analysis of the holes (vulnerabilities)

The analysis of the interviews and academic exercise revealed additional holes, or vulnerabilities, that could be considered in the model. It is important to point out that the number and types of holes changes constantly, depending on the context in which the model is implemented and the stakeholders informing the model. The vulnerabilities presented in Table 1 are high-level overarching holes; the third column suggests other potential holes developed through the academic workshop exercise but is not an exhaustive list.

Table 1 Additional holes for the consideration in the model

LINES OF DEFENCE[4]	VULNERABILITIES LISTED IN THE REPORT	OTHER POTENTIAL VULNERABILITIES
1.1 Asset condition data	• Older assets • Good quality asset data because of the fragmentation and evolution of supply-chain (and thus lack of accountability and responsibility) • Slow uptake of digitisation, automation and remote data sensing • Culture (optimisation of assets as a cost, not investment) • Barrier to data sharing (e.g. IP)	• Financial implications for collecting info on older assets • Conditions of older assets in close proximity
1.2 Incident reporting and dissemination of learnings	• Lack of collection and dissemination of information on failures and near misses • Unwillingness to share/ acknowledge mistakes • Financial disincentives • Legal disincentives • Lack of leadership in terms of sharing failures • Lack of environment in which staff can speak out	• Lack of knowledge continuity (e.g. due to changes in staff) • Lack of information on near-misses or small failures that do not lead to a complete failure • Who collects and reports the data? • Is the information about incidents easily accessible? • Ignoring other industries
1.3 CPD	• Weak system of enforcing CPD in a rapidly changing context	• Higher Education
2.1 Standards and regulations	• Regulation as the final aim rather than a process • Working to the spirit rather than to the letter of a standard • Out of date • Contradictory to one another and to what other industries want • Incomplete	• Replication of standards and regulations without proper adjustment to a context
2.2 Attention to quality in design and construction	• Lack of systematic application of the concept of inherent safety • Lack of safe-life • Lack of fail-safe • Poor quality construction • Poor quality maintenance • Focus on personal safety but not on quality on site • Tolerance to incidences of errors • Tolerance of incidences of defects • Organisational culture and attitudes towards quality • Lack of understanding by the importance of quality	

[4] Numbers in this column refer to the Lines of Defence, as illustrated in Figure 1.

LINES OF DEFENCE[4]	VULNERABILITIES LISTED IN THE REPORT	OTHER POTENTIAL VULNERABILITIES
2.3 Suitably qualified and experienced persons	• Lack of SQEP regime or equivalent • Lack of long term management of asset integrity	• Lack of engagement with wider range of stakeholders • Actions of those not appropriately/ professionally qualified
2.4 Code of professional conduct	• Growing specialisation of engineering • Growing commodification (difficult for a client to identify the engineering competence that they need) • Lack of adherence to the Code	
2.5 Client organisation	• Multiple interfaces and handover points • Badly executed interface management • Badly executed handovers • Siloed decision making • New or one-off clients/ clients without established reputation • Budgetary restraints (esp. for one-off clients on smaller projects)	• Lack of clients' awareness of the holes • Lack of collaboration among the whole team
3.1 Governance	• Project boards do not act as collective decision makers as they may not have relevant competencies to make an informed decision • Lack of a wide range of skills and expertise on the board • Safety treated as a priority (can change) rather than value (stays)	• Lack of the board's awareness of near misses
3.2 Investment cases and the H&S file	• Lack of demonstration of learning from past failures and near misses • Safety cases that set out risks and their causes are not routine • Poorly prepared safety files • Not up-to-date safety files • Safety files not passed on as part of asset handover	• Organisational culture
3.3 Independent scrutiny and assurance	• Self-certification • Self-accreditation • Self-insurance • Lack of independent scrutiny at all stages of DCOP	• Rapidly changing context • Actions of those not appropriately/ professionally qualified
3.4 Asset stewardship of infrastructure	• Engineer as a technical advisor rather than as a guiding mind • Lack of a guardian role • Lack of whole operation oversight	

The identification of the holes revealed some crosscutting influencers that could form a hole in every line of defence. These include: understanding of risks; asset handover; skills, knowledge, attitude, training and experience (SKATE); culture (value rather than a priority); breadth of stakeholder engagement; effective communication. However, during the exercise with the panel members these have been reduced to four crosscutting influencers and will be discussed in more detail in section 3.1, as it was deemed critical to keep the model as simple as possible, without reducing its meaningfulness.

The analysis of the holes also reveals complex links between lines of defence, when the increase or decrease in one hole may intentionally or unintentionally increase or decrease other holes (Figure 3).

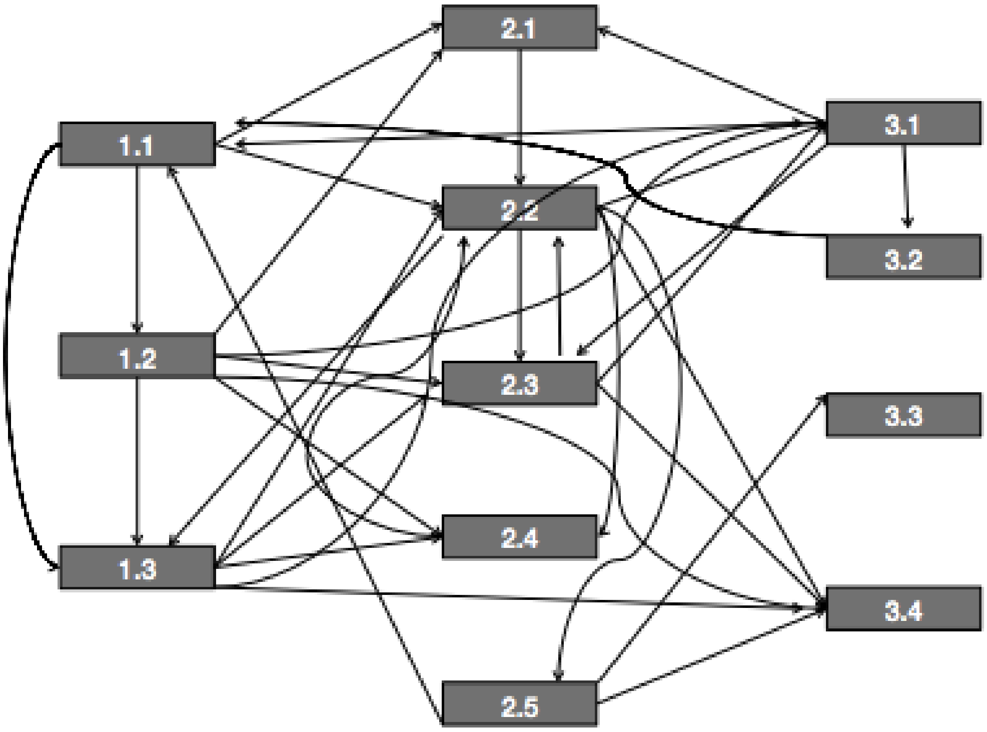


Figure 3 Conceptual interdependencies that demonstrate a non-linear relationship between the lines of defence

2.2 Gaps in the model

The academic exercise revealed further gaps in the model. It was agreed in the expert workshop that these cannot be added to the layers of defence, but should be considered when thinking about a broader context within which a failure may occur:

- ***Lack of explicit multi-hazard consideration***: current layers of defence do not consider an occurrence of two or more hazards/ threats happening at the same time. Often addressing different hazards and threats requires different measures – some of which may be conflicting (i.e. solutions to one problem can lead to further unforeseen problems).
- ***Lack of holistic consideration of risks***: the model is theoretical and thus does not explain how it can be implemented in a specific context, where it is critical to identify vulnerability of what and vulnerability to what that needs reducing.

- ***Lack of consideration of the impact that governance** (in its broadest sense) **has on systemic failure***: policy adjacency and the overall national policy framework (and rapid changes in it)
- ***Complexity of infrastructure assets***: different ownership, different scale of operation, different governance
- ***Engagement with wider range of stakeholders***, other professional bodies and non-members
- ***Post-incident response***, including reactions to an incident: whilst most of the post-incident response strategies are most likely to be kept confidential, it is critical to point out the importance of carrying out post-incident evaluation, in order to build back better.

3. Suggested changes

3.1 Crosscutting influencers

Through the exercise with the ICE panel members, four crosscutting influencers (i.e. factors that could affect every line of defence, positively or negatively) were confirmed; these include:

- *Understanding of risks*, including the perception of risks;
- *Culture*, making risk assessment value rather than a priority;
- Effective *communication* among the widest range of stakeholders;
- *Politics and legislation* (national and international political actions that may affect project's operation and maintenance, depending on budget cuts, ownership etc.):
  - most of the issues are systemic yet government decisions often affect the size of the holes regardless of the actions of the industry. The consideration of the model thus should be caveated in a way that includes policy, government decision and pressures from central government).

Crosscutting influences could be visualised as 'knock-out' holes in a 13amp electrical back-box (Figure 4); they are the 'threads' that run through all the plates. Good or bad thread practice will affect all plates in some way, in addition to lines of defence specific holes. The crosscutting influences can be seen as negative ('genetic vulnerabilities' that, if triggered, create holes in all lines of defence) and positive ('golden threads' that, if addressed, fill in some of the holes in all lines of defence). Following the logic of the Swiss Cheese Model and as demonstrated in Figure 4, some of the crosscutting issues will open and some will remain closed. However, in practise the holes can be partially open and may change their size as well as move randomly.

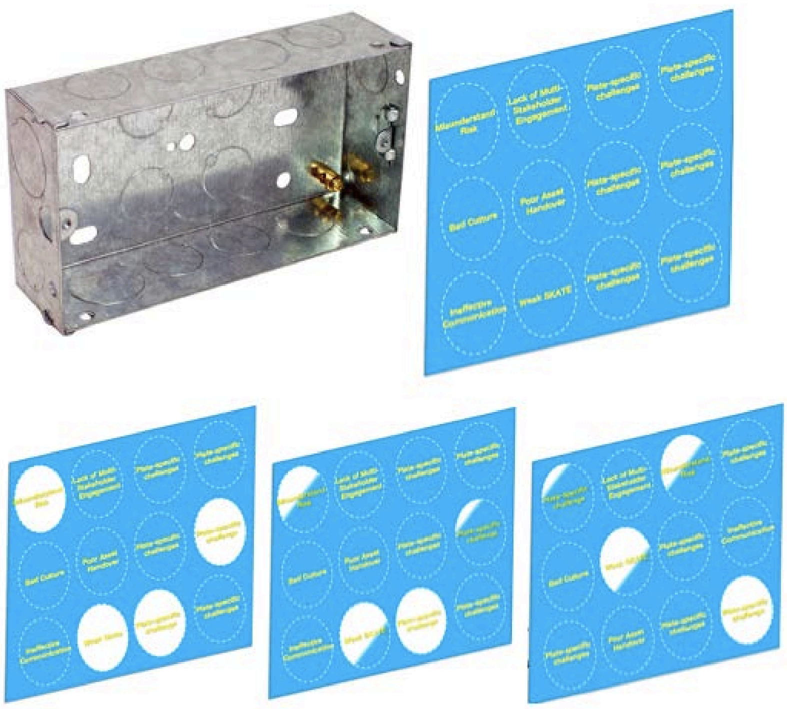

Misunderstand Risk
Lack of Multi-Stakeholder Engagement
Plate-specific challenges
Bad Culture
Poor Asset Handover
Ineffective Communication
Weak SKATE

Figure 4 Visual representation of crosscutting influencers on the lines of defence as 'knock-out holes'

3.2 Post-incident phase

It is suggested that post-incident considerations should be included in the model once the lines of defence are explored, by partially adapting the bowtie model (section 2). The post-incident phase covers consideration of responses immediately after an incident (and how an incident is handled), longer-term responses to an incident as well as mitigating strategies that could reduce the potential impact of an incident, and the future preventative strategies. This phase does not provide specific responses but instead encourages consideration of how to build back better. The bow-tie idea of post-incident response aids the understanding of ‘what can people do (or set up) *before* the project or *before* the incident to minimise the fall-out *if* the incident occurs’.

3.3 Setting the risk assessment context: resilience audit

More holistic approach to working through the model can be supported by the international risk management standard ISO 31000 ‘Risk management – Principles and guidelines ‘(British Standards Institution, 2009; 2011) presents four stages, those being risk identification, assessment, evaluation, and treatment. It is however suggested that the ‘treatment’ stage should be expanded into two stages, to aid end users to ‘identify’ what measures can be used, and to ‘prioritise’ them in relation to their effectiveness (see Bosher, 2014). The five key stages of such framework are detailed in Table 2 and should be considered prior to working through the lines of defence. Table 3 presents a checklist (and an example) that could be used to carry out a resilience audit; this can be carried out for a project as a whole or for each line of defence and each hole separately.

Understanding the potential impacts and likelihoods of vulnerabilities occurring lead to understanding the overall risks, therefore aiding the prioritisation of the risk reduction measures. For instance, it has been suggested by the members of the board that Lines 2.3 (SQEP) and 3.4 (Asset stewardship of infrastructure) should be considered as priority as they may set holes for other lines; this however is context specific and may change depending on a project.

Table 2 Detailed contents of the ISR Framework (Bosher 2014 after Mansfield et al. 1996)

Stage		Descriptor	
1	Identify, characterize, and assess hazards/threats	**Hazard/Threat identification –** the process of finding, recognising and describing hazards/threats to which the space is exposed. Hazard/Threat identification involves the identification of: • Type of hazard/threat • The events/circumstances when the hazard/threat is prevalent • Their causes • Their potential consequences It involves: • Assessing historical data, • seeking informed and expert opinions, and • understanding stakeholders' needs.	
2	Assess the vulnerability to specific hazards/threats	**Vulnerability assessment** is the process of assessing the susceptibility of the intrinsic properties (the structure, materials, construction, planning etc.) to a hazard/threat that can lead to an event with a consequence	
3	Determine the risk (i.e. the expected consequences of specific hazards/threats on specific assets)	**Identifying the level of risk** - magnitude of a risk or combination of risks, expressed in terms of the combination of the likelihood (chance of something happening) and the impact (consequences) of an incident caused by that hazard/threat. It utilises a **Risk Matrix** as a tool for ranking and displaying risks by defining ranges for consequence and likelihood	
4	Identify ways to reduce those risks (i.e. reduce the size of a hole)	**1. Inherent safety –** eliminate the possibility of hazards/threats occurring 2. **Prevention –** reduce the likelihood of hazards/threats 3. **Detection –** measures for early warning of hazards/threats 4. **Control –** limiting the size of the hazards/threats **5. Mitigation and adaptation –** protection from the effects of hazards/threats **6. Emergency response –** planning for evacuation and access for emergency services	**Identifying (and prioritising) a course of action to address and treat the hazard/threat and its associated risks**. Treatment can involve: • avoiding the risk by deciding not to start or continue with the activity that gives rise to the risk; • removing the hazard/threat source; • changing the likelihood or magnitude; • changing the consequences; • protecting assets/spaces from the effects of the risk • preparedness planning for the impacts of risks (events) • sharing the risk with another party or parties [including contracts and risk financing]; and • retaining the risk by informed decision making

Table 3 Resilience audit with an example developed during the expert workshop

Line of defence	**Holes**	**Potential impact of a vulnerability**	**Likelihood of the vulnerability appearing**	**Risk of a hole occurring**	**Ways of reducing vulnerability (examples)**
		1 to 5, with 1 = lowest impact and 5 = highest			
2.2 Attention to quality in design and construction	Lack of systematic application of the concept of inherent safety	5	1	Low	CPD
	Lack of safe-life	5	2	Low	
	Lack of fail-safe	5	2	Low	Technology
	Poor quality construction	5	4	High	Incentives
	Poor quality maintenance	5	4	High	
	Focus on personal safety but not on quality on site	*It was decided that this hole is not clearly defined in the interim report and should not be evaluated*			
	Tolerance to incidences of errors	5	4	High	Culture, incentives
	Tolerance of incidences of defects	5	4	High	Culture, CPD
	Organisational culture and attitudes towards quality	5	3	Medium	CPD, SQEP
	Complex supply chains	5	3	Medium	

4. Summary of the proposed changes to the model and recommendations

The proposed model is presented in Figure 5. It displays the links between the potential causes, vulnerabilities, preventative and mitigative controls and consequences of a major incident. The model does not find the answers but emphasises what is known but is not used and what is not known – and thus where the vulnerabilities are likely to make bigger 'holes' and lead to failures.

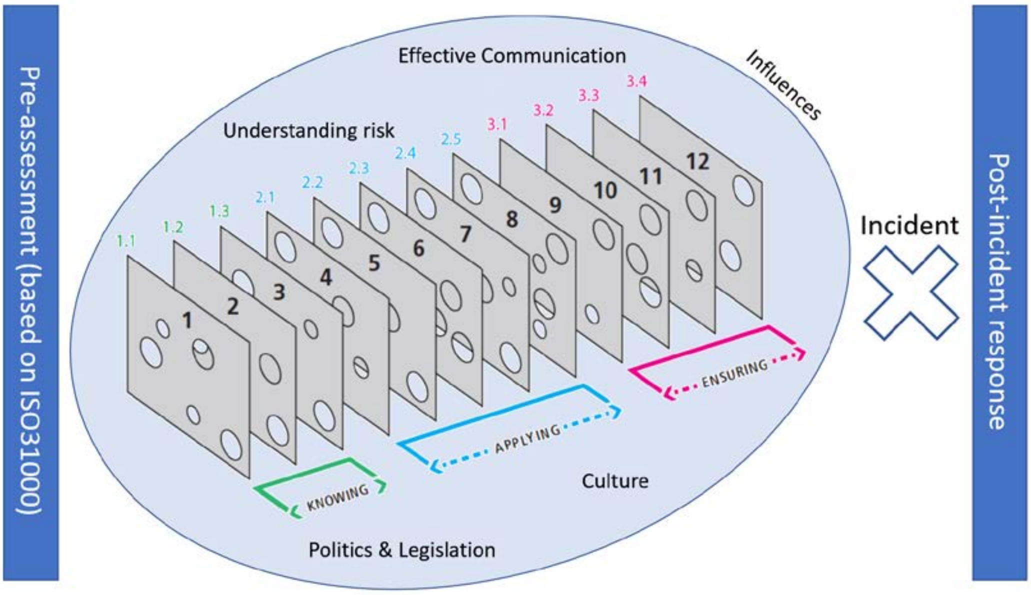


Figure 5 Proposed changed to the Lines of Defence: introducing holistic risk assessment, crosscutting influencers, and post-incident response

The proposed changes reflect the importance of understanding the overall risk context, crosscutting influences that may affect every line of defence, and post-incident response. In an ideal world, all the information would be available to proceed with the model, but in reality, informed guesses and trade-offs will have to be made. It is also crucial to consider broader societal and policy contexts when considering the model. It is however important to point out that this model presents a process that should be thought through on a regular basis, rather than treated as an end point, due to the changeable nature of the holes and influencers.

The following recommendations are proposed for the inclusion in the final report to make the model more accessible and effective for non-experts and those without specific/ prior knowledge of the industry:

1. Highlight that the model should be considered throughout a **lifetime of a project** (rather than as a one-off exercise) as depending on a changing context (e.g. ageing infrastructure) the holes in the lines of defence will also change; the model represents a process rather than an end point.
2. Define the **terminology** used in the report to avoid misinterpretation of the holes (e.g. safe-life; self-certification), and extend definitions where appropriate (e.g. 'false self-certification' and 'well-intentioned self-certification')

3. Highlight the **limitations** of the Swiss Cheese Model, in particular its linearity that does not allow reflecting complexity and interdependencies of and among the lines of defence.
4. Explore whether **prioiritisation** of the lines of defence is important and should be considered.
5. Consider which **stakeholders** (i.e. any persons with an interest or concern in a project) may provide relevant information
6. Assess the risks **holistically**, prior to identifying and reducing the holes in each line of defence
7. Explore potential tensions (will filling in one hole **create other holes?) and synergies** (will filling in one hole **close other holes?**) when considering risk reduction measures
8. Include **post-incident** considerations.

Although purely conceptual, the 12 Lines of Defence model enables considering lessons learned and highlighting the importance of larger societal context. It emphasises that lines of defence – and holes – are interconnected and interdepended.

Conclusion

This report presented an academic evaluation of the applicability and validity of the ICE’s 12 Lines of Defence model. The report concludes that the adaption of Reason’s Swiss Cheese Model as a basis of the Lines of Defence is appropriate, as it is well recognised and understood by a wide range of stakeholders. Notwithstanding, we have proposed an integration of post-incident analysis, appreciation for crosscutting influencers that could positively or negatively impact every line of defence, and a general risk management framework to be included in the model in order to increase and extend the reach of the model, without compromising its recognition and effectiveness. Clarifications on the limitations of the model, terminology used in the model and its applicability (i.e. consideration throughout the lifetime of the project) were also proposed.

References:

Abdelhamid, T.S. and Everett, J.G. (2000), Identifying root causes of construction accidents. *Journal of Construction Engineering and Management*, ASCE, 126 (1): 52-60.

Bosher L.S., (2014), Built-in resilience through Disaster Risk Reduction: Operational issues, *Building Research & Information*, 42 (2): 240-254

British Standards Institution (2009), Risk Management: Principles and Guidelines. London: British Standards Institution Group

British Standards Institution (2011), Risk Management: Code of Practice and Guidance for the Implementation of BS ISO 31000. London: British Standards Institution Group

Chmutina, K., Bosher, L., Coaffee, J. and Rowlands, R. (2014), Towards integrated security and resilience framework: a tool for decision-makers, *Procedia Economic and Finance*, 18: 25-32.

Loosemore, M. (1998), Psychology of accident prevention in the construction industry. *Journal of Management in Engineering*, 13 (3): 50-56.

Mansfield D., Poulter, L. and Kletz T.A., (1996), *Improving Inherent Safety*, HSE Books, Sudbury

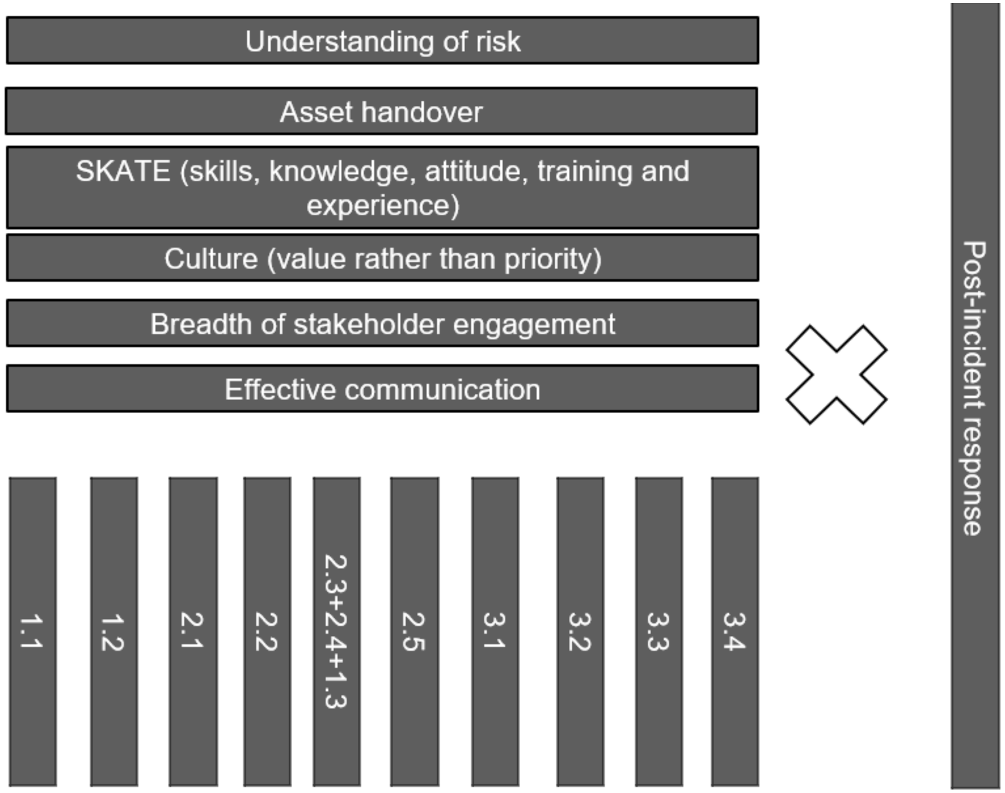
Petersen, D. (1996), *Human Error Reduction and Safety Management*, International Thompson Publishing, NY.

Reason, J (1990), *Human Error*, Cambridge University Press, Cambridge.

Suraji, A., Duff, A.R. and Peckitt, S,J, (2001), Development of a causal model of construction accidents causation. Journal of Construction Engineering and Management, ASCE, 127 (4): 337-344.

APPENDIX A

ICE In Plain Sight – academic validation exercise


Understanding of risk
Asset handover
SKATE (skills, knowledge, attitude, training and experience)
Culture (value rather than priority)
Breadth of stakeholder engagement
Effective communication
1.1
1.2
2.1
2.2
2.3+2.4+1.3
2.5
3.1
3.2
3.3
3.4
Post-incident response

In this exercise, you will be required to consider whether the cross-cutting issues, suggested by Loughborough University are truly cross-cutting. Overarching vulnerabilities are like ‘knock-out’ holes in a 13amp electrical back-box; they are the ‘threads’ that run through all the plates. Good or bad thread practice will affect all plates in some way. The cross-cutting issues can be seen as negative (‘genetic vulnerabilities’ that, if triggered, create holed in all lines of defence) and positive (‘golden threads’ that, if addressed, fill in the holes in all lines of defence).

The aim of the exercise is to understand whether the model supports holistic considerations that could help preventing the failure. The model does not find the answer but to emphasise what is known but is not used and what is not known – and thus where the vulnerabilities are likely to make ‘bigger holes’ and lead to failures. Whilst the exercise may seem long, you should not spend much time on it: please rely on your intelligent guess but highlight where the information is not easily available. Also consider where the information could be found.

The task

Choose an incident:

- Piper Alpha
- Buncefield
- Edinburgh schools

Using the information about the chosen incident (available in Appendix D and Appendix E of review of the In Plain Sight working group reports), map out (i.e. answer yes or no) the known and unknown information for the overarching vulnerabilities in the following table (based on the information that is easily accessible/ available + intelligent guess).

Cross-cutting vulnerabilities	***Would this vulnerability create a hole in every line of defence (that are not cross-cutting)?***	***Was this vulnerability known before the incident***	***Has this vulnerability become known after the incident?***	***If was not known, how to check that it exists (e.g. who would you need to talk to, what kind of information would you need)?***
Understanding of risk				
Asset handover				
SKATE (skills, knowledge, attitude, training and experience)				
Culture (value rather than priority)				
Breadth of stakeholder engagement				
Effective communication				