Protecting Critical Infrastructure by Adapting to Resilience Thinking for a National Blackout Risk Assessment Framework

M.A. van Harte, L. Pittorino, L. Mahumapelo, R. Koch, C. Masike, S. Joseph, G. Oosthuizen, R. Nkuna,
Eskom,
vhartem@eskom.co.za

1. ABSTRACT

Electricity infrastructure resilience of the South African power grid is challenging, considering the lack of generation support from our neighbouring countries in the event of a blackout incident [1]. A blackout incident is a very low-probability, high-impact incident and, in the context of this paper, refers to an event that results in the total disconnection of all generation sources from the transmission grid. Given this context, it is prudent for utilities to ensure that adequate treatment and control measures are in place to prevent a national blackout incident as well as to ensure their readiness to respond. Due to the complex nature of the various interdependencies among stakeholders, causes, controls, and treatments, the use of conventional integrated risk management techniques may result in only a superficial assessment being conducted.

The paper focuses on the application of the integrated risk assessment for the blackout planning to be undertaken when considering the safety barriers in the design, planning, operation and recovery. In this paper, the blackout objectives, description and bow-tie analysis techniques are utilised. The paper concluded with suggested blackout threat scenarios considering a national blackout bow-tie analysis.

2. INTRODUCTION

Electricity infrastructure has traditionally been classified as critical infrastructure due to its impact on other essential services (such as healthcare, telecommunications, security, etc.), which influences the well-being of the community, health, the economy, the environment, and national security [2]. Threats to the electricity infrastructure may lead to an interruption of supply and, in extreme cases, could result in a national blackout incident.

While it may be regarded as a rare incident (HILP), it is, nonetheless, prudent for a utility and the country to thoroughly plan and prepare to respond in a coordinated manner. This is of particular importance for utilities where there is limited available generation support from neighbouring countries, resulting in an increased complexity of restoring the national interconnected power system.

The interactions and reliance among the various sectors such as telecommunications, large industry, and government services (for example, security and health) will have an impact on the emergency response structures of the utility as well as the country[3].

In recent years, a number of studies have been conducted, evaluating the threats of terrorism, cyber-attack, and extreme storms [4]–[11]. Lessons learnt from previous international blackout incidents have provided an opportunity to assess the readiness of power utilities for similar events. However, as each interconnected power system is configured differently, it would require a separate and integrated risk assessment to review its specific vulnerabilities. Furthermore, it is clear that the electric power delivery system cannot be made completely impervious to harm from natural, space, and/or terrorist causes [12].

3. RESILIENCE THINKING IN POWER SYSTEM

Resilience is more than simply "the ability to bounce back" after a failure; an organisation seeking to be highly resilient needs to also continuously focus on aspects related to the potential for failure at all levels of the organisation [13]. The concept of resilience is becoming popular in the engineering, business, and natural science disciplines. It has led to interesting debate and attempts to define its role and scope in these different fraternities.

There are no universal resilience definitions, as this is a multifaceted concept that is defined in the context of the discipline/field [14], [15], [16]. For the purpose of our enquiry, we propose a "working definition" of resilience as described in ***Figure 1***.

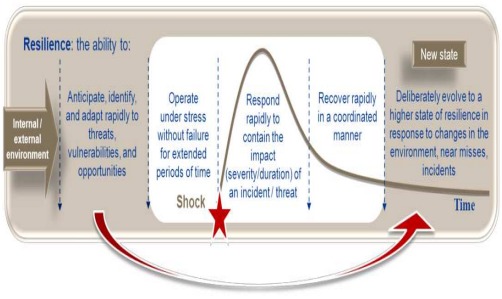

Figure 1: *A "working definition" of resilience*
(Source: Koch et al. [17]*)*

4. INTERNATIONAL BLACKOUT STUDIES

In recent years, the impact of natural and man-made hazards on critical infrastructure has resulted in governments elevating the requirements to enhance the ability of critical infrastructure to absorb, prevent, and/or respond appropriately to the disruption of essential services [18]–[20].

A review of international blackout incidents was conducted as part of the risk assessment. It was noted that similar studies [9], [11], [21]–[24] were not limited to blackout incidents (where there was a total loss of generation), but also included large transmission interruptions to load centres.

A review of the primary causes and/or contributing factors was done for 10 of the largest international blackout incidents, including the following:

Table 1: *Top 10 national blackouts, year versus impact*

Year	Country	People (million)
1999	Southern Brazil	**97**
2001	India	**230**
2003	North-east USA	**55**
2003	Italy	**55**
2005	Java – Bali	**100**
2009	Brazil and Paraguay	**87**
2012	India	**620**
2014	Bangladesh	**150**
2015	Pakistan	**140**
2015	Turkey	**70**

This review revealed that, in most cases, the triggers for the blackout were natural phenomena or plant failures. However, in many cases, additional defence mechanisms that ought to have prevented the incident from developing into a blackout were either not in place or were not effective.

From this initial study, anecdotally, the following were the primary causes of the blackouts that were reviewed (which could differ from the causes of the initial incident):

- Inability to monitor and control the power system
- Inability to cope with a sudden disconnection of multiple generators
- Generators being unable to cope with a sudden large loss of load
- Inability to adequately balance generation supply and customer demand
- Malicious intent of parties to disrupt utility functions
- Incorrect tripping of power system protection
- Unpredictable performance of plant due to deviations from design, operating, or maintenance criteria
- A severe natural event having an impact on several stations or lines that is outside their design capability

5. DISASTER MANAGEMENT ACT

Compliance with the requirements of relevant legislation, regulations, and licences obligates the electricity supply authority to plan and prepare for an extreme event such as a national blackout incident [25], [26]. Given these requirements, it is imperative that an electricity supply authority have an understanding of the mechanisms of failure and control measures to prevent and plans to respond to a major electricity incident(s).

In the case of South Africa, an organ of state is required to comply with the requirements of the Disaster Management Amendment Act (Act No. 16 of 2015) and to provide an integrated disaster management plan based on functional roles and responsibilities for major electricity-related incidents [25], [27]. The business objectives related to disaster management that inform disaster risk assessment and disaster risk reduction are based on the following categories: (i) *prevention of incidents or disasters*; (ii) *response to, and recovery from, an incident or disaster*; (iii) *business continuity requirements during an incident or disaster; and* (iv) *effective coordination between Eskom and external response partners and stakeholders.*

6. CRITICAL INFRASTRUCTURE

In March 2014 [2], a common narrative was concluded between five nations (the USA, the UK, Canada, Australia, and New Zealand) on the definition, approach, concept, and implementation in order to arrive at a shared understanding of critical infrastructure. The proposed definition formulated a starting point of collaboration among these nations:

"Critical infrastructure, also referred to as nationally significant infrastructure, can be broadly defined as the systems, assets, facilities and networks that provide essential services and are necessary for the national security, economic security, prosperity, and health and safety of their respective nations."

It includes the establishment of government departments and/or institutions to assist these nations to manage risks to their critical infrastructure by developing a shared understanding of security and resilience capabilities. These nations recognised "*resilience as the need for systems to have the capacity to be*

vhartem@eskom.co.za

flexible and adaptable to changing conditions, both foreseeable and unexpected, and to be able to recover rapidly from disruption".

In this context, the energy sector (which *includes electricity infrastructure*) has been identified as critical infrastructure. The means that the resilience capabilities in this sector should be able to adapt to changing conditions and withstand and recover rapidly from a disruption. Therefore, assessing the readiness and defining the risk framework for a national blackout are imperatives for all developed and developing nations.

6.1. Interdependencies of critical infrastructure

In recent years, unprecedented and singular disaster incidents (such as the 9/11 terrorist attack) have revealed the interdependencies of critical infrastructure. These consequences can be attributed to complex interrelationships, dependencies, and interdependent cross sectors due to the interconnected nature of the relationship between critical infrastructures and essential services [3].

Rinaldi et al. (2001) [28] proposed some of the earliest descriptive interdependency types, namely, (i) physical, (ii) cyber, (iii) geographic, and (iv) logical. The fundamental definition of infrastructure interdependency and its modelling has led to further distinction among first-, second-, and third-order dependencies. Figure 2 provides an example of the multiple connections of critical infrastructure as a "system of systems", which has multiple points and a bidirectional relationship.

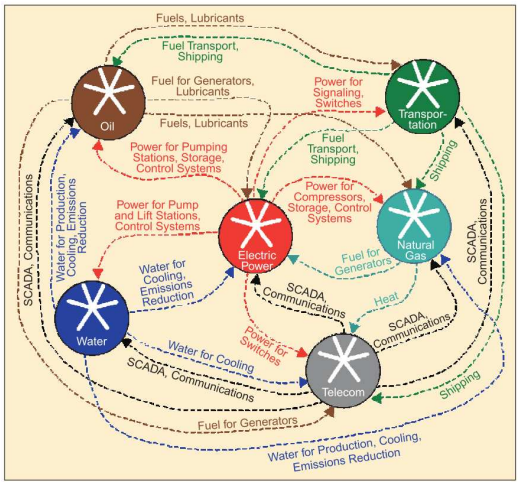

Figure 2: *Examples of infrastructure interdependencies (Source: Rinaldi et al.* [28]*)*

Given the example above, it is clear that there is a growing need to develop assessment techniques to analyse and better understand the interconnected chain of influence among cross sectors [37], [38].

7. INTEGRATED RISK MANAGEMENT

In terms of the ISO 31000 standard [31], a quantitative risk assessment (QRA) includes establishment of the context, risk identification, performance of the risk analysis, and risk evaluation [32], [33]. The aim of managing the risk is to achieve an appropriate balance between realising opportunities for gains and minimising adverse impacts. The Eskom[1] Integrated Risk Management (IRM) Policy and Standards require that risk management be incorporated in decision-making. Eskom aims to embed risk management in all of Eskom's critical business processes in order to ensure that risks are identified and managed prior to an incident occurring that may prevent it from achieving its objectives. Given the adoption of a risk-intelligent approach, Van Harte et al., 2011 [32], suggested a procedure for evaluating transmission system risks using the integrated risk management methodology described in the new ISO 31000 risk management standard.

When performing an integrated risk assessment for a national blackout incident, the primary objective is that of preventing an incident from occurring. Once a national blackout incident has commenced, the objective is to minimise the severity of the blackout and to maximise the speed of system restoration in a safe manner. Furthermore, as a blackout incident has a major impact on various industries and consumers at both a provincial and a national level, the risk assessment needs to also consider coordinated response and recovery mechanisms with government institutions and large industry.

Traditionally, where controls are deemed to be effective, no further action is generally required. However, a new development in the risk management fraternity in Eskom is that all the existing controls identified to manage a particular risk now need to be separately evaluated in terms of their level of effectiveness in managing the risk. The control rating is evaluated against the following: non-existent, totally ineffective, ineffective, partially effective, and fully effective. Each control that is evaluated and found to be less than fully effective needs to be further developed through performing new tasks on controls in order to bring them to a level of being fully effective.

One of the challenges of treating a blackout risk is developing an understanding that controls are interdependent on external factors that may change over time, thereby compromising the adequacy and effectiveness of the control. This can be achieved

1 *Eskom is a vertically integrated, South African, state-owned electricity company, established in 1923. The utility is the largest producer of electricity in Africa and is among the top seven utilities in the world in terms of generation capacity and among the top nine in terms of sales. (www.eskom.co.za)*

vhartem@eskom.co.za

by assessing the governance and compliance and by auditing the controls in order to understand their adequacy and effectiveness.

Furthermore, there are some enablers to ensuring that an effective risk assessment process is adopted to achieve the blackout risk objectives, namely:

- *clear understanding of causes and controls of the causes;*
- *identification of critical processes and dependencies; and*
- *ensuring effective stakeholder engagement.*

8. BLACKOUT RISK

A national blackout remains a high-impact low-probability (HILP) disaster scenario, given the various system safety barriers that are in place to prevent this.

In the context of this paper, a working definition of a national blackout has been formulated to create a context and set boundaries for the risk assessment:

"[T]he complete de-energisation of the interconnected power system where some generators may have islanded to house load, leading to all customers losing supply."

Therefore, a national blackout incident is a total loss of power throughout the country and is the most severe form of interruption of supply that customers may experience, lasting from a few hours to possibly weeks after the incident.

8.1 Blackout risk objectives

In terms of ISO 31000 [31], risk is traditionally defined as the

"[e]ffect of uncertainty on objectives"

Regarding the uncertainty of the outcome of objectives, Van Harte et al. [1] argue that there are different blackout planning roles to establish the appropriate resilience capabilities (*absorptive, adaptive, and restorative capabilities*) in the event of a national blackout incident, namely:

- **core:** *blackout prevention, response, and recovery normally led by the System Operator;*
- **company:** *organisational response and business continuity;*
- **country:** *collaborative planning and response at national, provincial, and local level; and*
- **regional:** *collaborative planning and response across neighbouring states.*

The various blackout planning roles form the basis of determining the integrated risk management business objectives in the external and internal context. The risk assessment will include a review of the causes, controls, and treatment plans to achieve success in terms of the identified objectives. **Figure 3** illustrates the four blackout risk objectives against the various blackout preparedness planning roles required for a national blackout incident.

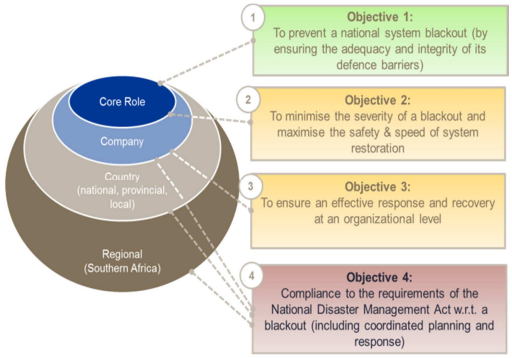

Figure 3: *Blackout risk objectives against the blackout planning roles*

8.2. Blackout risk description

The most likely cause of a national blackout would be an unforeseen sequence of events that results in a cascading collapse of the transmission/generation system, leading to a complete loss of electricity supply across the country. Such an event can occur with very little or even no warning.

8.3 Blackout bow-tie analysis

In terms of ISO 31010 [34], this risk assessment technique analyses the chain of events, from causes to consequences, by demonstrating the causal relationships in high-risk scenarios. It provides a visual representation of plausible accident scenarios, considering the trigger incident "hazard", by mapping the threat to "top event" and consequence if all the controls are breached. The relationship among the undesirable event, its causes, accidental scenarios, and the preventive and treatment measures to limit its consequences is demonstrated using this technique. The "Swiss cheese" barrier model (also known as the accident causation model) [17] is another technique utilised to evaluate primary and secondary barrier effectiveness by clustering the barriers in the following: *(i) engineering; (ii) formal; (iii) oversight; and (iv) behaviour.*

A "hazard" leads to an initiating incident(s), which – if not adequately contained – will increase the likelihood of a national blackout. Such threats may arise from internal sources (for example, equipment failure, human error, etc.) and/or from external sources (for example, severe storms, terrorism, etc.). Internal trigger scenarios need to be evaluated considering a broad range of threat characteristics and vulnerabilities for both the steady and the dynamic state of the interconnected power system. The external trigger scenarios are normally evaluated and documented in the integrated disaster management plan, considering that their planning, response, and recovery are normally coordinated at a national or provincial level and may be beyond

vhartem@eskom.co.za

the utility's core mandate (for example, an external trigger incident such as terrorism is normally led by the state security or defence force). In such a case, the System Operator would be in a position to alert the country emergency response structures of a potential threat to the interconnected power system.

Figure 4 illustrates the bow-tie risk analysis technique as described in [34], considering the defence and recovery safety barrier mechanisms. The aim of the bow-tie technique is to identify control measures that a utility should consider that are in place to prevent and recover from a national blackout incident. It considers the mechanisms to prevent a blackout incident, controls and contains causes and consequences that may lead to it, and/or manages the restoration of the interconnected power system after a national blackout incident. The adequacy of these safety barriers can be different, depending on the threat scenario that they control and should be operational when they are required. Therefore, the effectiveness of these barriers should be evaluated against the adequacy and reliability of the controls due to the fact that each barrier has unintended intermittent weaknesses. Therefore, the identification of the escalation factors and controls should consider the factors that prevent or minimise the possibility of the defence and recovery barrier mechanisms from becoming ineffective.

The application of this technique has been employed to systematically assess, enhance, integrate, and exercise the resilience of the interconnected power system in the event of a national blackout incident [17]. These safety barrier mechanisms are evaluated against the core blackout risk objectives for before, during, and – in certain cases – after the national blackout incident.

The defence mechanisms consist of a number of barriers that would attempt to contain and/or eliminate the causes introduced by the initiating trigger/incident. The defence barrier mechanisms in the fault tree are classified through the following safety barriers:

- **Design:** *Grid Code requirements, governance committees, and planning and design standards.*
- **Asset management:** *life-cycle management and renewal, maintain-to-design base, and spares management.*
- **Operating:** *manual load shedding, automatic protection systems, operating reserves, operate-to-design base, and outage management.*

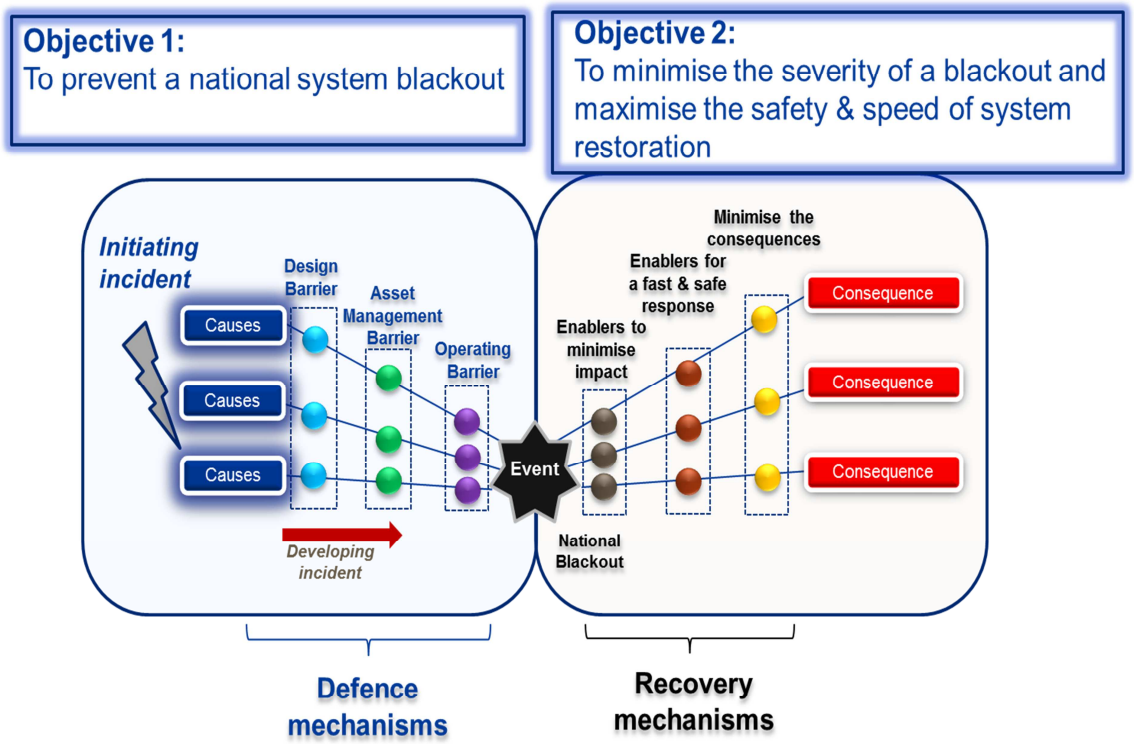

Figure 4: *Bow-tie risk visualisation for blackout defence and recovery mechanisms*

vhartem@eskom.co.za

As a developing event penetrates the different barriers and exceeds their safety margin, it may lead to a cascading incident, resulting in instability of the power system, with the disconnection of generating units and customer load.

After the "top/critical event", namely, a national blackout incident, the response barrier mechanisms consist of a number of barriers that contain the impact and enable a quicker restoration of the generator units as well as coordination of response and recovery of the interconnected power system [ ]. The recovery barrier mechanisms in the event tree are classified according to the following safety barriers:

- **Reaction to minimise impact:** *islanding scheme, governance activation, system status, and emergency response structures.*
- **Response to contain:** *black-start facilities and restoration plan to restart the power system.*
- **Recovery plans:** *reconnecting essential and critical loads and re-establishing the interconnected power system.*

9. BLACKOUT THREAT SCENARIOS

The resilience of the electricity infrastructure involves a complex system, with interconnected chains of influence between systems and bidirectional relationships [6, 7]. These interdependencies create a source for threat scenarios, considering the interaction between systems. Thus, ignoring the interdependencies between critical systems will lead to an incomplete understanding and a lack of resilience investment.

Given these blind spots, the bow-tie analysis assists in determining the blackout threat scenarios that are inherent in the planning, design, maintenance, and operation of these critical systems. It provides the indispensable tool to identify "*what can go wrong*" and "*how it can go wrong*" and is an important aspect of risk intelligence.

Furthermore, in providing assurance against these threats, the following should be considered during the assessment of complex risk:

- **Governance:** *are the identified controls incorporated in existing governance committees/structures?*
- **Risk:** *what are the known risks associated with the identified control? If there are risks associated with the control, are these risks reflected in the relevant risk register?*
- **Compliance:** *what compliance breaches have occurred, and is the control effective, or is further enhancement of the control required?*
- **Audits:** *have any external audits been performed on this control? If so, please state when the last audit was conducted.*

Table 2 summarises the potential threat scenarios that may lead to a trigger incident (as informed by international blackout events) and possible breach scenarios of the safety barriers, as identified during the bow-tie risk analysis for a national blackout incident.

Table 2: *Description of threat scenarios for a national blackout incident*

Threat scenarios	What is the exposure for this threat?
Lack or loss of power system visibility and control	Loss of SCADA visibility (situational awareness) will make monitoring, controlling, and balancing supply/demand on the power system very difficult.
Multiple-unit tripping (assuming low/inadequate reserves)	Sudden loss of generating capacity and, especially, escalation of multi-unit trips (MUTs) and loss of multiple stations will inevitably result in a severe shortage of generating capacity, likely greater than the norm that can be covered through load shedding, leading to possible brown-outs or, ultimately, a system blackout.
Generator inadequate response to high-frequency events	Inadequate or slow response to sudden increases in frequency could result in "sympathy" tripping of single or multiple generating units, with resultant network frequency fluctuations and triggering of escalation of multi-unit trips to loss of multiple stations.
Inadequate response to low/under-frequency events	Inadequate system reserves and response capability, or inappropriate utilisation of these, could result in instantaneous and evolving system instability, leading to brown-outs or blackouts. The interconnected power system is not able to adequately balance generation supply and customer demand.
Malicious intent of parties to disrupt utility operations by means of electronic warfare	Cyber-attacks on critical systems (IT and OT systems) could have an impact on business and operational systems.
Cascaded network tripping (uncleared network faults)	Incorrect system tripping can result in multiple circuits being unavailable, having an impact on the supply-demand balance.
Unpredictable performance of generating plant	Governance processes are designed to ensure compliance and conduct reviews of the risks

vhartem@eskom.co.za

Threat scenarios	What is the exposure for this threat?
due to deviations from design criteria	to maintain the design base of the generation fleet.
Generation plant not being maintained and/or operated as intended	Maintenance and operating standards are defined, and independent reviews exist; the risk is non-adherence as well as the inspection regime not being complied with.
System instability due to inadequate transmission planning and design	Designs that are not robust can introduce a risk in terms of supply-demand balance during a network incident or may initiate a blackout incident due to plant failure.
Transmission plant and system not being operated and/or maintained as intended	Inappropriate response from the System Operator to ensure adequate reserves/ineffective outage management/excessive risk taking/inappropriate operator response to a system alarm or incident could lead to a blackout.
Fault(s)/event(s) that cause a situation to exceed the design parameters of plant (for example, solar storms, severe weather, etc.)	There is the risk of multiple transmission assets tripping for a common cause, resulting in various vulnerabilities and challenges in maintaining the supply/demand balance.

Note: *table not entirely complete and represents only the salient Blackout threats scenarios.*

10. CONCLUSION

A major electricity-related incident can, therefore, have a significant impact on a country [36]. It requires the electricity sector to pursue resilience strategies by developing capabilities to absorb, prevent, and/or respond appropriately to the disruption of critical infrastructure. The reliability and resilience of such critical interdependent infrastructure are crucial to the well-being of society, security, and the economy. Thus, the paper anecdotally discussed the primary causes of the top international blackout incidents and provided the context of compliance for any responsible utility. It also discussed integrated risk management in a utility setting.

A bow-tie analysis technique was used for the risk assessment to identify the potential threat scenarios and their causes and consequences, as well as to evaluate the barriers and controls [37]. The application of the technique provides a visual representation of the cause-consequence chain for identifying relevant threat scenarios and safety barriers required. This technique is similar to the "defence-in-depth" analysis technique adopted in the nuclear industry to evaluate safety barriers and may include engineered controls, formal controls (work procedures, etc.), management assurance and oversight controls, and organisational culture controls [17].

The concept of infrastructure interdependency modelling was also discussed to provide a basic setting for establishing blackout risk objectives in different planning roles for planning and readiness assessment to recover rapidly from an extreme event such as a national blackout. In addition, the paper unpacked the application of an integrated risk management assessment technique, namely, bow-tie analysis. Also discussed was the concept of the defence and recovery barriers that ought to be considered during blackout readiness assessment. This paper provided a framework for understanding the vulnerability of, and threats to, electricity infrastructure, considering planning roles against blackout risk objectives. The framework started by understanding the controls and their effectiveness, to be evaluated by fault tree analysis, the cause of the event, and the event tree, analysing the consequences to determine the threat scenarios to be considered during planning and readiness for a national blackout incident.

The paper concluded with a description of blackout threat scenarios for a national blackout incident for any utility to consider during planning, design, maintenance, and operations.

11. ACKNOWLEDGMENTS

The authors acknowledge the co-authors and Eskom National Blackout Working Group for their contribution, guidance, and support.

12. REFERENCES

[1] M. . Van Harte, R. Koch, A. Nambiar, G. Hurford, T. Smit, S. Joseph, G. Loedolff, and U. Heideman, "Infrastructure Resilience: Regional and National Blackout Planning," in *CIGRE - Southern Africa Regional Conference*, 2015.

[2] New Zealand Treasury, "Critical 5 - Forging a Common Understanding for Critical Infrastructure Shared Narrative," 2014.

[3] D. D. Dudenhoeffer, M. R. Permann, and C. Miller, "Interdependency Modeling and Emergency Response," pp. 1230–1237, 2007.

vhartem@eskom.co.za

[4] W. Lu, Y. Bésanger, E. Zamaï, and D. Radu, “Blackouts : Description , Analysis and Classification,” pp. 429–434, 2006.
[5] M. Bruch, M. Kuhn, and G. Schmid, “Power Blackout Risks,” *Cro Forum*, no. November, p. 32, 2011.
[6] L. Zhang and L. Sun, “Multi-objective service restoration for blackout of distribution system with distributed generators based on Multi-agent GA,” *Energy Procedia*, vol. 12, pp. 253–262, 2011.
[7] J. F. Shortle, “Efficient simulation of blackout probabilities using splitting,” *Int. J. Electr. Power Energy Syst.*, vol. 44, no. 1, pp. 743–751, 2013.
[8] S. D. Anagnostatos, C. D. Halevidis, A. D. Polykrati, P. D. Bourkas, and C. G. Karagiannopoulos, “Examination of the 2006 blackout in Kefallonia Island, Greece,” *Int. J. Electr. Power Energy Syst.*, vol. 49, no. 1, pp. 122–127, 2013.
[9] J. J. Wong, C. T. Su, C. S. Liu, and C. L. Chang, “Study on the 729 blackout in the Taiwan power system,” *Int. J. Electr. Power Energy Syst.*, vol. 29, no. 8, pp. 589–599, 2007.
[10] E. Policy, “Large blackouts in North America : Historical trends and policy implications Large Blackouts in North America : Historical trends and policy implications,” no. December 2009, 2014.
[11] P. Hines, J. Apt, and S. Talukdar, “Large blackouts in North America: Historical trends and policy implications,” *Energy Policy*, vol. 37, no. 12, pp. 5249–5259, 2009.
[12] Bernice Lee, Felix Preston, and Gemma Green, “Preparing for High-impact, Low-probability Events: Lessons from Eyjafjallajökull,” 2012.
[13] M. . Van Harte, R. Koch, and G. Rohde, “Building System Resilience through Multi-Disciplinary and Cross Divisional Regional Resilience Teams,” in *CIRED*, 2011, no. 594, pp. 6–9.
[14] G. Kasthurirangan and P. Srinivas, *Sustainable and Resilient Critical Infrastructure Systems*. Scientific Publishing Services Pvt. Ltd, 2010.
[15] D. E. Alexander, “Resilience and disaster risk reduction : an etymological journey,” in *National Hazards Earth System Science*, 2013, pp. 2707–2716.
[16] R. Sanchis and R. Poler, *Definition of a framework to support strategic decisions to improve Enterprise Resilience*, vol. 46, no. 9. IFAC, 2013.
[17] R. . Koch, M. . Van Harte, A. J. Correia, and S. . Van Der Merwe, “Power System Resilience : A Conceptual Framework South Africa,” in *CIGRE - Southern Africa Regional Conference*, 2013, no. October, pp. 1–12.
[18] UK Cabinet Office, “Keeping the Country Running: Natural Hazards and Infrastructure,” UK, 2011.
[19] A. R. Berkeley Iii, M. Wallace, and NIAC, “A Framework for Establishing Critical Infrastructure Resilience Goals: Final Report and Recommendations,” National Infrastructure Advisory Council, 2010.
[20] A. Government, “Critical Infrastructure Resilience Strategy: Plan,” 2010.
[21] Z. Bo, O. Shaojie, Z. Jianhua, S. Hui, W. Geng, and Z. Ming, “An analysis of previous blackouts in the world: Lessons for China’s power industry,” *Renew. Sustain. Energy Rev.*, vol. 42, pp. 1151–1163, 2015.
[22] M. Panteli, “Impact of ICT Reliability and Situation Awareness on Power System Blackouts,” *[Thesis]. Manchester, UK Univ. Manchester; 2013.*, 2013.
[23] P. Hines, J. Apt, and S. Talukdar, “Trends in the history of large blackouts in the United States,” *IEEE Power Energy Soc. 2008 Gen. Meet. Convers. Deliv. Electr. Energy 21st Century, PES*, vol. 15213, pp. 1–8, 2008.
[24] A. Stefanini and M. Masera, “Electric System vulnerabilities : a state of the art of defense technologies,” 2006.
[25] National Disaster Management Advisory Forum, *Disater Management Amendment Act*. Republic of South Africa: NDMC, 2015.
[26] T. South and A. Grid, “The South African Grid Code The System Operation Code,” no. July, pp. 1–21, 2010.
[27] National Disaster Management Centre, *A policy framework for disaster risk management in South Africa*, vol. 7, no. 1. South Africa: NDMC, 2000, p. 131.
[28] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, “Identifying, understanding, and analyzing critical infrastructure interdependencies,” *IEEE Control Syst. Mag.*, vol. 21, no. 6, pp. 11–25, 2001.
[29] P. Pederson, D. Dudenhoeffer, S. Hartley, and M. Permann, “Critical infrastructure interdependency modeling: a survey of US and international research,” *Idaho Natl. Lab.*, no. August, pp. 1–20, 2006.
[30] M. Ouyang, “Review on modeling and simulation of interdependent critical infrastructure systems,” *Reliab. Eng. Syst. Saf.*, vol. 121, pp. 43–60, 2014.
[31] ISO, *Risk management — Principles and guidelines*. London: ISO, 2010.

vhartem@eskom.co.za

[32] M. . Van Harte, R. . Koch, M. Nene, G. Havford, and M. Bala, “Integrated Risk Management and System Adequacy Assessment: Implementation of the ISO 31000:2009 Standard in the South African Power System,” in *CIGRE Symposium*, 2011, no. April, pp. 1–5.

[33] Alexei Sidorenko, “Four key concepts for effective risk management,” *Continuity Central*, 2016. [Online]. Available: http://www.continuitycentral.com/index.php/news/erm-news/1402-four-key-concepts-for-effective-risk-management. [Accessed: 16-Sep-2016].

[34] ISO/IEC, *Risk management — Risk assessment techniques*, vol. 2009. London: ISO/IEC, 2009.

[35] A. Atef and O. Moselhi, “Understanding the effect of interdependency and vulnerability on the performance of civil infrastructure,” 2013.

[36] M. . Van Harte, R. Koch, U. Heideman, S. Mahomed, T. Moganedi, and J. Correia, “Planning for Major Electricity-related Incidents,” in *DMISA - Disaster Risk Reduction 2016*, 2016.

[37] V. Villa, N. Paltrinieri, F. Khan, and V. Cozzani, “Towards dynamic risk analysis: A review of the risk assessment approach and its limitations in the chemical process industry,” *Saf. Sci.*, vol. 89, pp. 77–93, 2016.

vhartem@eskom.co.za