# A Bayesian Network Approach for the Quantitative Assessment of Resilience of Critical Systems

T.V. Santhosh

*Institute for Risk and Uncertainty, University of Liverpool, Liverpool, UK.*
*Bhabha Atomic Research Centre, Mumbai, India. E-mail: s.santhosh@liverpool.ac.uk*

Edoardo Patelli

*Centre for Intelligent Infrastructure, University of Strathclyde, Glasgow, UK.*
*Institute for Risk and Uncertainty, University of Liverpool, Liverpool, UK. E-mail: edoardo.patelli@strath.ac.uk*

The major accidents in industry, and failures of critical infrastructure have triggered an absolute need for new and efficient approaches in risk assessment and safety management. Resilience engineering has attracted widespread interest as it presents a whole new approach to measuring and maintaining the safety of critical systems. In this paper, an integrated framework is proposed for resilience assessment of critical systems under various threat scenarios using Bayesian network. This new approach addresses all the factors associated with resilience principles together with the dynamic interactions of a system during threats. Quantitative resilience metrics are proposed to provide new insights on the importance of different factors within the resilience framework and optimise the mitigation and recovery phases. The approach is applied to assess the resilience of safety system of a nuclear reactor.

*Keywords*: Resilience, human and organizational factors, critical infrastructure, Bayesian networks, safety.

## 1. Introduction

The traditional risk assessment is no longer adequate to effectively analyze and manage the risks associated with critical infrastructures (Qureshi, 2007). Recently, the human factor engineering and resilience engineering has attracted widespread interest from various industries as well as academia as it presents altogether a new approach to measuring the resilience and maintaining the safety in critical infrastructures (Shirali, 2013). This new approach focuses on how to help the operators to cope with complex situations under pressure to successfully mitigate the threats. Quantitative researches, especially in the process industries, nuclear industry remained relatively undeveloped in the field of resilience engineering. In addition, resilience metrics are very limited (e.g. Erol, 2010) or incomplete, i.e. we can only measure the potential for resilience but not the resilience itself (Woods, 2006).

There is no universally agreed definition of resilience engineering but it involves a set of factors associated with resilience principles namely, anticipation, response, learning and monitoring (Pillay, 2017). Most of the work on human and organizational factors, and resilience engineering involved qualitative investigations from the data collected through field observations, audit reports, virtual experiments and expert elicitation (Lay, 2015; Musharraf, 2018). The situation awareness and mental workload are found to be the key factors in determining the performance of operator during dynamic threat scenarios (Burtscher, 2012), and the conventional human reliability analysis (HRA) methods fail to address such dynamic behavioural changes of operator during the unexpected threats. Moreover, the performance shaping factors (PSFs) used to evaluate the operator's performance may vary significantly with respect to the impact of the threat (Morais, 2020).

This research proposes an integrated framework for quantitative assessment of system resilience under severe threat scenarios. The proposed approach employs the computational intelligence techniques to incorporate the dynamic behavioural changes of human and organizational factors together with the dynamic interaction of critical infrastructure system into a resilience model of the threat scenario. This improved approach addresses all the factors associated with resilience principles (Azadeh, 2014) and presents system resilience profiles for decision making. The modelling involves both expected and unexpected threat scenarios under extreme conditions. The threats triggered by natural disasters such as earthquakes, Tsunami or man-made threats such as physical or cyber-attacks are considered in the modelling (Tolo, 2019). Bayesian networks are employed to model the critical system under expected or unexpected threat scenario (Garg, 2017; Yodo, 2017).

The proposed framework is applied to a safety related system of a nuclear reactor to demonstrate the capability and applicability of the method. The approach will present the entire analysis as an integrated model of the threat considering all the elements of resilience principles including available safety functions

*Proceedings of the 30th European Safety and Reliability Conference and the 15th Probabilistic Safety Assessment and Management Conference*
*Edited by* Piero Baraldi, Francesco Di Maio and Enrico Zio
*Published by* Research Publishing, Singapore.
ISBN: 978-981-14-8593-0; doi:10.3850/978-981-14-8593-0

for recovery upon disruptive event. The paper describes the key aspects necessary to analyze resilience for disruptive state, recovery with effective resilience strategy. The proposed approach is generic enough and can be applied to any kind of critical infrastructure system.

## 2. Resilience and Evaluation Methodology

Resilience is the ability of a system to recover from a disturbance so that it can sustain required operations under both expected and unexpected threat scenarios (Cai, 2018). The concept of resilience has been evolved from various fields including ecology, economics, psychology, and sociology, and the research in the field of engineering is very limited in comparison with that in non-engineering areas (Fang, 2016; Hosseini, 2016b). Rocchetta et al. (2018, 2020) have assessed the resilience of repairable power grids by subjecting to weather-induced failures with data deficiency. The American Society of Mechanical Engineers defines resilience as the capability of a system to sustain external and internal disruptions without discontinuity of performing the system function or, if the function is disconnected, to fully recover the functions rapidly (ASME, 2009). Haimes et al. (2009) defined resilience as the capability of the system to withstand a major disruption within acceptable degradation parameters, and recover within an acceptable time and composite costs and risks. Many researchers have proposed their own resilience definitions from different perspectives (Woods, 2006; Yodo, 2016). Based on the definitions, various resilience metrics and their corresponding evaluation methodologies have also been developed (Henry, 2012; Ouyang, 2012).

Although several resilience metrics are currently available, quantifying the resilience of a specific system remains a serious challenge due to many factors involved in such metrics. All these definitions and metrics strongly rely on the overlapping concepts of resilience such as adaptability, robustness, redundancy, flexibility, survivability, recoverability, rapidity, and resourcefulness (Filippini, 2014; Woods, 2015). Resilience is considered to be an intrinsic capability and an inherent attribute of a system itself. The structure of the system determines performance related properties, such as robustness, adaptability, redundancy, flexibility, and survivability, whereas the maintenance resource determines the time-related properties, such as reparability, recoverability, rapidity, and resourcefulness (Cai, 2018; Christopher, 2014). Similarly, the external factors, such as disturbance, attack, and disaster events are not the intrinsic properties of resilience and hence not involved in the resilience metric. Hence, the structure and maintenance resource in the system form an integrated model of resilience measure.

### *2.1 Resilience principles*

Resilience is generally understood as the ability of a system to recover from a disruptive event. Resilience engineering attempts to manage and understand performance variability and addresses efficiency, safety and resilience as emergent properties. Thus, the focus of resilience engineering is on resilient performance, rather resilience as a property of the organization. In a resilient organization or system, six main items have been identified. Each item has a special description in different application fields. Regarding performance management and safety, the six principles as a reference to quantitative assessment of resilience engineering are top management commitment, reporting culture, learning, awareness, preparedness and flexibility (Hollnagel, 2006, 2008).

### *2.2 System resilience*

A resilient infrastructure system can have various performance states when subjected to unanticipated internal or external disturbances as shown in Figure 1 (Zhang, 2018). The system resilience can be quantified by a performance measure which can be any quantifiable metric such as reliability, availability, etc. (Cai, 2018).

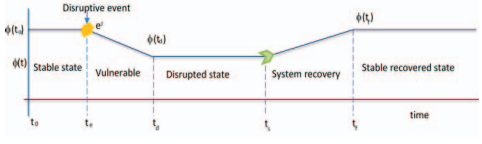


Fig. 1. Concept of resilience

Barker et al. (2013) describe resilience as the ratio of system recovery at time t to the loss suffered by the system at some previous point in time $t_d$. If $R_{es}(t)$ denote the resilience of a system at time t, then the resilience of an infrastructure system is expressed by the following equation:

$$R_{es}(t) = \frac{Recovery(t)}{Loss(t_d)}, t \geq t_d \qquad (1)$$

As shown in Figure 1, $\varphi(t_0)$ represents the value of the system performance function corresponding to the stable state. The performance is expected to remain at this level until the occurrence of the disruptive event $e^j$ at time $t_e$. Once the disruptive event $e^j$ occurs, the performance degrades gradually until it converges to a stable disrupted state at time $t_d$, and the corresponding system performance

value of the disrupted state is $\varphi(t_d)$, which is lower than the original value $\varphi(t_0)$. During the time period $t_s$–$t_d$, the situation of the disruptive state of the system is assessed and necessary recovery action is initiated at time $t_s$, which restores the system from the disrupted state to a new stable recovered state with system performance function value $\varphi(t_f)$ at time $t_f$. Based on this discussion, the resilience of a system from a performance metric is defined as (Henry, 2012):

$$R_{es}(t_f|e^j) = \frac{\varphi(t_f|e^j) - \varphi(t_d|e^j)}{\varphi(t_0) - \varphi(t_d|e^j)}, \forall e^j \in D \quad (2)$$

Where, D is a set of disruptive events.

### *2.3 Availability as resilience metric*

Every infrastructure system has its own performance metrics such as reliability, availability, maintainability, safety. For a continuously operating systems or infrastructure the widely accepted measure is availability over reliability as the system is usually restored after a disruptive event. Referring to Figure 1, $\varphi(t)$ can be treated as availability of the system which in turn is a measure of performance. The availability of a system reaches to a steady-state value after period of time from the initial start-up upon implementation of successful operational and maintenance tasks. This state of operation is referred to as stable state with highest availability until time $t_e$ where disruptive event occurs. Upon the occurrence of internal or external disruptive event $e^j$ at time $t_e$, the availability decreases gradually and converges to a maximum disrupted state over time $t_d$, and remains in this state until the restoration takes place. During the time period $t_s$-$t_d$, all the efforts are made by the staff in terms of assessing the fault situation, allocating the necessary resources and logistics, identifying the suitable crew for repair actions, etc. Once a successful restoration is implemented at time $t_s$, the availability starts increasing gradually and reaches to a new stable recovery state at time $t_f$ and continue to perform in this state until the occurrence of further disruptive events. This process of maintaining an infrastructure system in a regular operational state subjected to several disruptive events accords with the property of resilience (Cai, 2018). Thus, resilience can be quantified with an appropriate resilience metric such as availability.

Based on this concept a framework has been proposed in this paper which integrates the resilience principles in modelling and satisfy the property of resilience. The schematic diagram depicting various factors involved in resilience modelling of a complex system is shown in Figure 2. As shown in Figure 2, the proposed approach models the system resilience taking into account all the resilience principles together with the recovery process under a threat scenario, and provides flexibility to achieve the required resilience by optimizing control variables such as human and organizational factors, maintenance aspects, etc. The approach presents a complete resilience model of an infrastructure system under any internal or external threat including cyber threats. As seen from the proposed framework, resilience modelling involves many aspects including the human factors, organizational factors, component operational states, maintenance aspects and spare part inventory in addition to other resources required to restore the system.

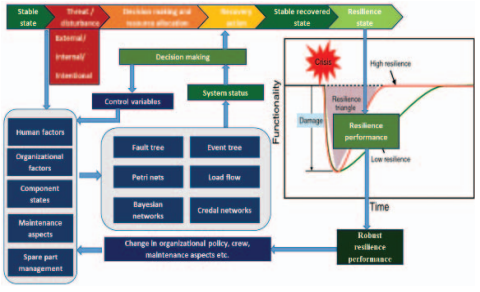


Fig. 2. Resilience modelling framework

The proposed approach computes the resilience of an overall system that is achieved from various individual factors which highly influence in getting a desired resilience profile. Apart from the internal or external disturbance on the system a large number of internal factors affects the system restoration. Amongst many factors, human and organizational factors are found to be most potential contributors towards achieving an effective resilience of the system (Reinerman-Jones, 2019), and hence they are called as control variables. With a set of these control variables under a threat, a proper modelling of the system provides an insight into decision making with regard to system restoration. These control variables may be adjusted with respect to high and low resilience requirements which largely depends upon the type and severity of the threat, and available resources. In addition, the maintenance aspects and spare part management highly influences the restoration plans. Once the system is restored it is important to assess the system performance after recovery which generally expected to be lower than the initial original performance due to changes in the failure and repair rates of replaced or repaired components,

redundancy structure, etc. In order to achieve the recovery performance as close to as original performance with highest resilience goals, an organization can undergo policy changes in terms of resource allocation, crew management and effective decision making. Thus, it necessitates to build a robust resilience model of the overall system under threat and provides a means to gain the maximum availability factor from an infrastructure system. In this study, we use availability as measure of performance for quantification of resilience (Henry, 2012). As can be seen from Equation (2), the value of resilience increases with the increase in availability.

### *2.4 System recovery*

Recovery actions enable a system to respond to unexpected disruptions. Well implemented recovery actions may sometimes improve capabilities of the system relative to its normal operating condition (Tran, 2017; Taleb, 2013). Such actions include repairing an affected system and adapting or reconfiguring an existing system structure. As most systems require the involvement of the human operators and strict adherence to organizational policies for repair or reconfiguration and eventually restoration of the system, human and organizational factors play an important role in the recovery phase. Other factors that affects the restoration efficiency are the maintenance related aspects, spare part availability, etc. which are well within the scope of organization management and can be improved. However, the human factors are highly complex to determine and may significantly change with respect to the type of disruptive event and progressive scenarios of the event (Kim, 2018). The resilience of the system depends upon the successful restoration and subsequent delivery of the expected performance.

The proposed framework uses availability as system performance measure to quantify the resilience. Since the temporal aspects of a system's response to disruptive events play significant role in resilience (Tran, 2017), the assessment of availability over time is used which is assumed to be in line with the restoration process such that they can be represented as time dependent resilience. This assumption enables the use of time series methods for analyzing a system's performance response. As the threats are random and some are unknown and operators have not been trained for such events, the human factor data with regard to recovery actions may not be available. Hence, use of simulator data or expert judgement is recommended in the absence of actual observed data (Morais, 2020; Yochan, 2018; Musharraf, 2014). The recovery probabilities for the restoration phase of the system upon a disturbance are generated through the available generic resources taking into consideration the highest possible situation awareness and lowest mental workload factors for best resilience requirements. The human operators with good situation awareness skills can properly assess the threat situation and take efficient corrective actions which greatly improves the resilience of the system (Hwang, 2008; Salmon, 2006; Hosseini, 2016a). The other important factor is the physical and mental workload which is a measurement of both physical and mental demands of an operator during an emergency situation (Song, 2013).

## 3. Case Study and Results

In order to illustrate the proposed method as an integrated framework, a safety related reactor regulation system of advanced thermal nuclear reactor is analyzed. The main function of the regulation system is to regulate the control rods so as to maintain reactor under normal operating conditions. This system consists of three different control rods namely, regulation rods, shim rods and absorber rods (Sinha, 2006). Regulating rods are used for reactor regulation, shim rods are used for reactor setback and absorber rods are used for Xenon override. The operation of these control rods is based on 2-out-of-3 sensor logic signal. The normal operation of an nuclear power plant depends upon the availability of regulation function, heat removal function and neutron moderation function with all other associated resources including power supplies. These functions are modelled together with a threat on sensor circuit using dynamic Bayesian network to demonstrate the resilience of the overall system. In the absence of exact probabilities, the Credal networks, similar to Bayesian networks, allows to model the interval probabilities (Estrada-Lugo, 2019, 2020) and implemented into OpenCossan software (Patelli, 2018). The parameter of interest for assessing the resilience is the steady state availability of reactor system comprising the regulating function, heat removal function and moderator function with associated power supplies. Internal, External or Cyber threat on sensor logic are postulated and resilience profiles generated. Internal threat may be an intentional by an insider or a random failure of the sensor itself. Any threat on sensor logic may result into malfunctioning of the regulating system which, if not mitigated, eventually leads to loss of regulation accident (LORA). Several threat scenarios are postulated based on the available safety and redundancy measures within the regulation system to demonstrate

various resilience sequences exhibited from the system.

The threat scenario is described as follows: One of the three sensors is affected by an internal threat. Since the functioning of regulation system depends on 2-out-of-3 logic the failure of one sensor is not going to affect the system much. However, the redundancy is lost and utility is expected to initiate the necessary actions or measures to remove the threat and restore the system back to normal operation within the predefined time. It is expected that upon the failure of one of the three sensors, the automatic setback function is initiated to limit the reactor power within the set limits so as to carry out the recovery operations. During this time period, the threat situation is assessed and system is restored to normal working mode. In the event of automatic setback being not actuated, the manual setback is initiated by an operator. In the unlikely scenario of failure of both automatic and manual setback functions the mitigation and restoration are entirely dependent upon the available safety systems and human intervention. Depending upon the resulting threat scenario the resilience sequence evolves accordingly. All the basic component models used in the modelling and quantification are the availability models, hence the resultant metric of the overall model remains availability of reactor system. The Bayesian model of the reactor system for various performance states under an internal threat on sensor circuit with an auto setback function working is shown in Figure 3 and the Bayesian model of the reactor system when system is restored after a disruptive event is shown in Figure 4. The failure and repair data for various components to quantify the resilience metric is taken from generic data source IAEA Tecdoc 478 (1988) and the performance shaping factors required for assessing the situation awareness and mental workload are taken from NUREG-6949 (2007).

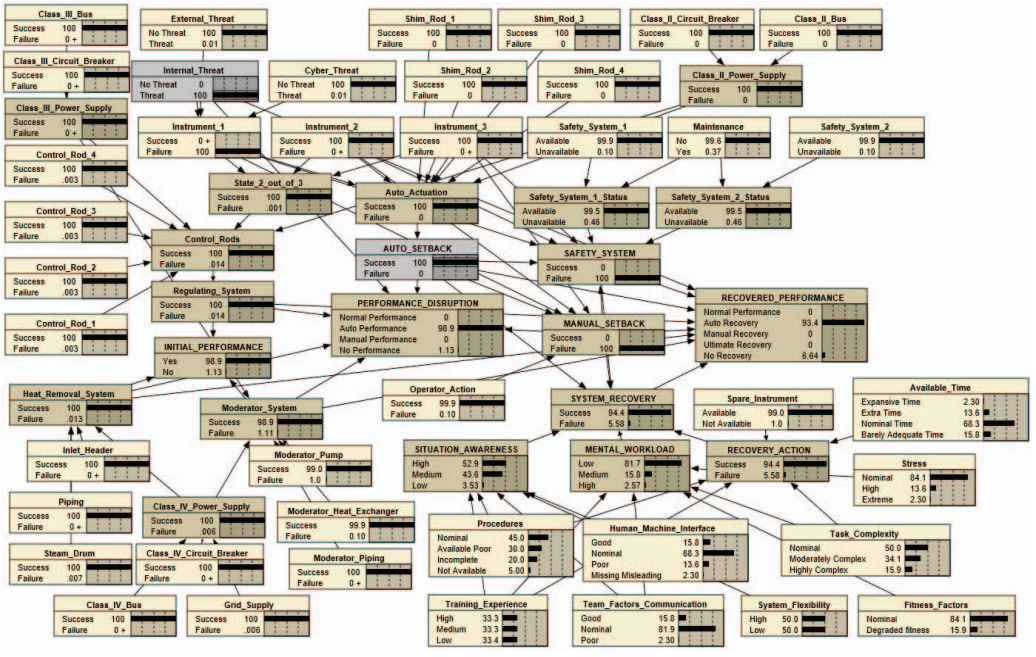


Fig. 3. Bayesian model with an internal threat and auto setback working

As the threat is on one sensor of a 2-out-of-3 sensor circuit, the performance of the system is not affected much due to redundant setback functions with highest component availabilities. During auto setback working, the availability reduces to 93.2 from initial 98.9. However, when restoration takes place, which implies the threat has been removed on the affected item with repair or replacement actions, the system regains to its maximum performance state which is shown in Figure 4. The other possible sequences such as failure of auto setback function, and a complete setback failure, which is very unlikely, are also

simulated in the dynamic Bayesian model under threat for a duration of one hour. In a complete setback failure scenario, the performance of the system degrades to its minimum and calls for a restoration after a complete shutdown which depends upon the availability of safety systems, spare parts if required etc. The resilience profiles with availability as resilience metric for these scenarios are shown in Figure 5. It is observed from Figure 5 that the restoration time depends on the available safety functions and, human and organizational factors.

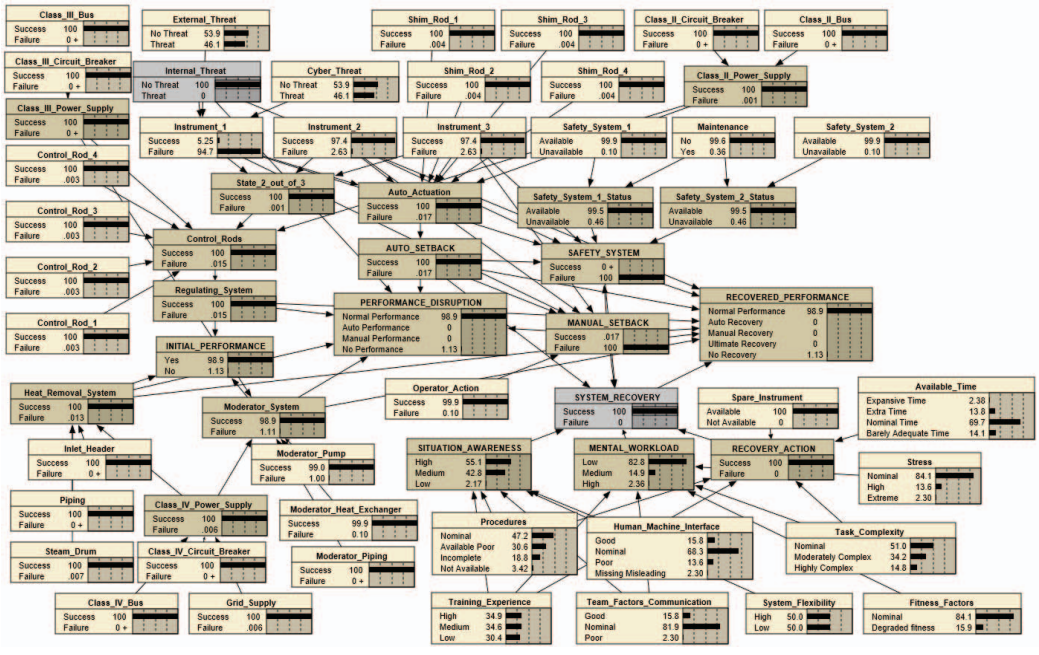


Fig. 4. Bayesian model with restoration after a disruptive event

It is logical to state that the chances of restoring the system is quite high when auto setback is working. However, when both auto setback and manual setback fail, the restoration might take longer time as it all depends on the availability of ultimate safety systems taking into consideration their maintenance aspects as well. When threat affects more than one sensor, the resilience profile takes the form similar to the one during a complete setback failure, however the restoration time can significantly change due to high severity of the threat.

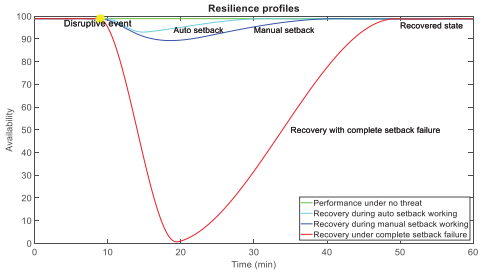


Fig. 5. Resilience profiles under a threat

## 4. Conclusions

The proposed approach is applied to a safety related system of a nuclear reactor to assess the resilience under a potential internal threat and the resilience profiles over the entire threat and recovery phase have been generated. The proposed framework integrates all the resilience aspects into a complete threat model of the reactor system and quantifies the availability as resilience metric. The dynamic Bayesian model of the reactor system captures all the dependencies including the human and organizational factors together with dynamic interaction of the system required for restoration. The approach presented in this study is flexible enough for simulating various kinds of threats and generating the possible resilience sequences existing within the system with optimal human and organizational factors. The quantitative resilience metrics of the reactor system under a threat provides insights on the importance of different factors to decision making process in terms of the resources within the system and for probable improvements to build more resilience.

**Acknowledgement**

This work has been supported by the UK Engineering and Physical Sciences Research Council (EPSRC) with the project entitled "A Resilience Modelling Framework for Improved Nuclear Safety (NuRes)", Grant No. EP/R020588/2.

**References**

ASME (2009). All-Hazards risk and resilience: prioritizing critical infrastructures using the RAMCAP Plus SM approach. *American Society of Mechanical Engineers (US).*

Azadeh, A., Salehi, V. (2014). Modelling and optimizing efficiency gap between managers and operators in integrated resilient systems: The case of a petrochemical plant. *Process Safety and Environmental Protection 92*, 766–778.

Barker Kash, Jose Emmanuel Ramirez-Marquez, Claudio M. Rocco (2013). Resilience-based network component importance measures. *Reliability Engineering and System Safety 117*, 89–97.

Burtscher Michael J., Tanja Manser (2012). Team mental models and their potential to improve teamwork and safety: A review and implications for future research in healthcare. *Safety Science 50* 1344–1354.

Cai Baoping, Min Xie, Yonghong Liu, Yiliu Liu, Qiang Feng (2018). Availability-based engineering resilience metric and its corresponding evaluation methodology. *Reliability Engineering and System Safety 172*, 216–224.

Christopher W. Zobel, Lara Khansa (2014). Characterizing multi-event disaster resilience. *Computers & Operations Research 42,* 83–94.

Erol Ozgur, Brian J. Sauser and Mo Mansouri (2010). A framework for investigation into extended enterprise resilience. *Enterprise Information Systems Vol. 4, No. 2,* 111–136.

Estrada-Lugo, H. D., Tolo, S., Angelis, M. de, Patelli, E. (2019). Pseudo credal networks for inference with probability interval. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems Part B: Mechanical Engineering 5,* 041010. https://doi.org/10.1115/1.4044239.

Estrada-Lugo, H.D., Santhosh, T.V., Patelli, E. (2020), An approach for resilience assessment of safety critical systems using credal networks. *in: ESREL/PSAM.*

Fang Yi-Ping, Nicola Pedroni, and Enrico Zio (2016). Resilience-based component importance measures for critical infrastructure network systems. *IEEE Transactions on Reliability, Vol. 65, No. 2*, 502-512.

Filippini Roberto, Andrés Silva (2014). A modelling framework for the resilience analysis of networked systems-of-systems based on functional dependencies. *Reliability Engineering and System Safety 125,* 82–91.

Garg, V., Santhosh, T. V., Antony, P. D. and Gopika V. (2017). Development of a BN framework for human reliability analysis through virtual simulation. *Life Cycle Reliability and Safety Engineering 6,* 223–233.

Haimes, Y. Y. (2009). On the definition of resilience in systems. *Risk Analysis, 29, 4.*

Henry, D., Jose Emmanuel Ramirez-Marquez (2012). Generic metrics and quantitative approaches for system resilience as a function of time. *Reliability Engineering and System Safety 99,* 114–122.

Hollnagel, E. (2006). Resilience: The challenge of the unstable. In: Hollnagel, E., Woods, D. D. & Leveson, N. C. (Eds.), *Resilience engineering: Concepts and precepts (p. 9-18).* Aldershot, UK: Ashgate.

Hollnagel, E., Nemeth, C.P., Dekker, S. (2008). Resilience engineering perspectives: Remaining sensitive to the possibility of failure. *Ashgate Publishing Ltd.*

Hosseini Seyedmohsen, Kash Barker (2016a). A Bayesian network model for resilience-based supplier selection. *Int. J. Production Economics 180,* 68–87.

Hosseini Seyedmohsen, Kash Barker, Jose E. Ramirez-Marquez (2016b). A review of definitions and measures of system resilience. *Reliability Engineering and System Safety 145,* 47–61.

Hwang Sheue-Ling, Yi-Jan Yau, Yu-Ting Lin, Jun-Hao Chen, Tsun-Hung Huang, Tzu-Chung Yenn, Chong-Cheng Hsu (2008). Predicting work performance in nuclear power plants. *Safety Science 46,* 1115–1124.

IAEA Tecdoc 478 (1988). Component reliability data for use in probabilistic safety assessment. *IAEA*, Vienna.

Kim Yochan, Jinkyun Park, Wondea Jung, Sun Yeong Choi, Seunghwan Kim (2018). Estimating the quantitative relation between PSFs and HEPs from full-scope simulator data. *Reliability Engineering and System Safety 173,* 12–22.

Lay, E., M. Branlat, Z. Woods (2015). A practitioner's experiences operationalizing, resilience engineering. *Reliability Engineering and System Safety 141,* 63–73.

Morais, C., Moura, R., Beer, M., Patelli, E. (2020). Analysis and estimation of human error from report of major accident investigations. *ASCE-ASME Journal of Risk and Uncertainty in Engineering Systems Part B: Mechanical Engineering 6* 011014.

Musharraf Mashrura, David Bradbury-Squires, Faisal Khan, Brian Veitch, Scott Mac Kinnon, Syed Imtiaz (2014). A virtual experimental technique for data collection for a Bayesian network approach to human reliability analysis. *Reliability Engineering and System Safety 132*, 1–8.

Musharraf Mashrura, Jennifer Smith, Faisal Khan, Brian Veitch, Scott MacKinnon (2018). Incorporating individual differences in human

reliability analysis: An extension to the virtual experimental technique, *Safety Science 107,* 216–223.

NUREG/CR-6949 (2007). The employment of empirical data and Bayesian methods in human reliability analysis: A feasibility study. *U.S. Nuclear Regulatory Commission.*

Ouyang Min, Leonardo Dueñas-Osorio, Xing Min (2012). A three-stage resilience analysis framework for urban infrastructure systems. *Structural Safety 36–37*, 23–31.

Patelli, E., Tolo, S., George-Williams, H., Sadeghi, J., Rocchetta, R., Angelis, M.D., Broggi, M. (2018). OpenCossan 2.0: An efficient computational toolbox for risk, reliability and resilience analysis. *in: Proceedings of the Joint ICVRAM ISUMA UNCERTAINTIES Conference.*

Pillay Manikam (2017). Resilience engineering: An integrative review of fundamental concepts and directions for future research in safety management, *Open Journal of Safety Science and Technology 7* 129-160.

Qureshi Zahid H. (2007). A review of accident modelling approaches for complex socio-technical systems, *12th Australian Workshop on Safety Related Programmable Systems (SCS'07),* Adelaide.

Reinerman-Jones, L. E., Niav Hughesb, Amy D'Agostino, Gerald Matthews (2019). Human performance metrics for the nuclear domain: A tool for evaluating measures of workload, situation awareness and teamwork. *International Journal of Industrial Ergonomics 69*, 217–227.

Rocchetta, R., Patelli, E. (2020). A post-contingency power flow emulator for generalized probabilistic risks assessment of power grids, *Reliability Engineering and System Safety 197,* https://doi.org/10.1016/j.ress.2020.106817.

Rocchetta, R., Zio, E., Patelli, E. (2018). A power-flow emulator approach for resilience assessment of repairable power grids subject to weather-induced failures and data deficiency. *Applied Energy 210.*

Salmon Paul, Neville Stanton, Guy Walker, Damian Green (2006). Situation awareness measurement: A review of applicability for C4i environments. *Applied Ergonomics 37,* 225–238.

Shirali, Gh. A., I. Mohammadfam, V. Ebrahimipour (2013). A new method for quantitative assessment of resilience engineering by PCA and NT approach: A case study in a process industry. *Reliability Engineering and System Safety 119,* 88–94.

Sinha, R. K., A. Kakodkar (2006). Design and development of the AHWR—the Indian thorium fuelled innovative nuclear reactor. *Nuclear Engineering and Design 236,* 683–700.

Song Bomi, Changyong Lee, Yongtae Park (2013). Assessing the risks of service failures based on ripple effects: A Bayesian network approach. *Int. J. Production Economics 141*, 493–504.

Taleb, N. N. and R. Douady (2013). Mathematical definition, mapping, and detection of (anti)fragility. *Quantitative Finance 13:11*, 1677-1689.

Tolo Silvia, John Andrews (2019). Nuclear facilities and cyber threats. *Proceedings of the 29th European Safety and Reliability Conference.*

Tran, H. T., Michael Balchanos, Jean Charles Domerçant, Dimitri N. Mavris (2017). A framework for the quantitative assessment of performance-based system resilience. *Reliability Engineering and System Safety 158,* 73–84.

Woods, D. D. (2006). Essential characteristics of resilience. *In: Hollnagel E, Woods D, Leveson N, editors. Resilience engineering: concepts and precepts. Burlington, VT: Ashgate Publishing Company.*

Woods, D. D. (2015). Four concepts for resilience and the implications for the future of resilience engineering. *Reliability Engineering and System Safety, 141* 5–9.

Yodo Nita, Pingfeng Wang (2016). Resilience modeling and quantification for engineered systems using Bayesian networks. *Journal of Mechanical Design 138*/031404-1-12.

Yodo Nita, Pingfeng Wang (2017). Predictive resilience analysis of complex systems using dynamic Bayesian networks. *IEEE Transactions on Reliability 66, No. 3*, 761-770.

Zhang Xiaoge, Sankaran Mahadevan, Shankar Sankararaman, Kai Goebel (2018). Resilience-based network design under uncertainty. *Reliability Engineering and System Safety 169*, 364–379.