A Resilience Evaluation Framework for Complex and Critical Systems

Santhosh TV

Institute for Risk and Uncertainty, University of 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, UK.
E-mail: edoardo.patelli@strath.ac.uk

Critical systems pose serious safety and reliability challenges for the researchers and practitioners when subjected to disruptive events. The complexity and uncertainty of threat prompts for consideration of resilience in system design and performance evaluation. Consequently, researchers have proposed several definitions and evaluation methodologies to assess resilience of potentially complex infrastructure systems. However, methods to quantify resilience of a specific infrastructure from multiple recovery paths, and their applicability to a large-scale system are limited. This paper presents a novel resilience evaluation framework to model critical infrastructure systems and to quantify net resilience by focusing on key characteristics of resilience. The proposed approach extends the framework proposed previously by the authors which explicitly models the temporal aspects of system response to disruptive event towards effective recovery from various recovery measures. This extended framework also proposes a global resilience model to quantify net resilience from multiple restoration paths based on the weighted geometric mean of area under multiple restoration curves. The proposed framework is illustrated with a case study on regulating function of nuclear reactor modelled using Petri nets. The model of the reactor system comprising regulating function, setback function, and human and organizational aspects is developed and simulated starting from an initial steady state until complete recovery state after a disruptive event on regulating rods. The net resilience of regulation system is computed from the performance parameter over various recovery sequences with their associated weights. This novel approach demonstrates its capability to be applicable to various critical infrastructure systems by considering temporal aspects of system with human and organizational factors for quantitative resilience evaluation.

Keywords: Resilience, human factors, critical infrastructure, nuclear power plant, Petri net.

1. Introduction

The increasing complexity in highly technological systems such as process industries, aviation, and nuclear industry is leading to potentially disastrous failure modes and a new kind of safety challenges (Shirali, 2013). The impact of nuclear power plant accidents has been proved by the Chernobyl, Three Mile Island and the Fukushima nuclear disasters (Zhao, 2020). Hence, safety and reliability of such complex engineering systems is significant important in order to maintain the risk within the acceptable limits and to protect the public and environment. The conventional risk and reliability techniques are well suited and widely employed to assess the system safety. However, such conventional techniques lack dealing with the dynamic system behaviour due to component failures or configuration changes thus failing to accurately represent the time dependent performance state. Recently, resilience engineering has attracted widespread interest from various industries as well as academia as it presents a whole new approach to measuring and maintaining the safety of infrastructure systems. Although resilience is often confused with reliability and robustness, resilience measures the inherent ability of a complex system to adapt, mitigate and to recover from expected or unexpected threat scenarios. However, the real challenge in resilience engineering occurs when such complex systems change their dynamic stability states into instability states.

Most of the work on resilience engineering deals with qualitative investigations from the data collected through field observations, audit reports and expert elicitation (Lay et al., 2015; Musharraf, et al. 2018). Human and organizational factors are claimed to be the key parameters in the evaluation of the safety of critical infrastructure. In particular, human factor plays a significant role in all stages of industrial processes. The statistics of industrial accidents indicate that the main factor of at least 66% and more than 90% of the incidents in different industries is attributed to human errors (Stellman, 1998). For example, in the tragic accidents such as nuclear accident at Three Mile Island, the space shuttle challenger explosion and Chernobyl nuclear accident, human errors have been known as the main cause (Azadeh, 2016). The maintenance aspects, spare parts inventory, dynamic system interactions together with human and organizational factors also play a fundamental role in real complex problems (George-Williams, 2018). Although the concept of resilience

Proceedings of the 31st European Safety and Reliability Conference
Edited by Bruno Castanier, Marko Cepin, David Bigaud, and Christophe Berenguer

ISBN: 978-981-18-2016-8; doi:10.3850/978-981-18-2016-8_357-cd

engineering is already applied in various areas, there are limited studies which specifically focus on how to measure resilience engineering in the safety context. Therefore, there is a gap in assessing resilience by quantitative methods with specific focus on multiple recovery sequences arising out of possible design capabilities.

This paper presents a novel framework for resilience assessment of complex engineering systems subjected to various threats to compute the net resilience from multiple recovery sequences. The proposed approach extends existing framework (Santhosh and Patelli, 2021) by explicitly models the temporal aspects of system response to disruptive event towards effective recovery from various recovery measures. Current approaches for assessing resilience consider many of the foundational aspects of resilience, such as absorption, restoration, and adaptation. This paper extends those approaches by addressing additional aspects of critical infrastructure including all the factors associated with resilience principles together with the dynamic interactions of a system during threat and provides quantitative resilience metric. The proposed approach is applied to a safety related system of a nuclear reactor to assess its resilience under a potential threat. The resilience profiles over the entire threat and recovery phase have been generated and net resilience computed from the performance parameter which is availability in this study.

2. Reliability, Safety, Resilience and Performance

The main challenge of any safety critical infrastructure to demonstrate its safety under different known and unknown threats. In particular, in nuclear industry important goal is to ensure the safety of public and its workers by keeping radiation exposure from the facilities as low as reasonably achievable during normal operations as well as during accidental conditions (IAEA SSG3, 2010). In order to meet this safety goal, the requirement of safety analysis has become mandatory for all the nuclear and non-reactor nuclear facilities. Safety analysis of critical infrastructure is aimed at the evaluation of risk from the facility and compliance to the regulatory requirements. It is based on both deterministic and probabilistic studies. In the deterministic safety analysis, only maximum credible accidents are considered, whereas probabilistic safety analysis covers all possible accident scenarios and their quantification in terms of release frequency and consequences. In both the methods, reliability and safety are the crucial parameters as the safe operation ensures the protection of public, environment, operational staff, and the facility itself whereas the reliable operation ensures the increased production time and reduced downtime cost.

A system with high reliability need not always be safe and vice versa. For example, safety is more crucial in case of nuclear industry whereas the reliability or performance may be more important in a production industry where it is less hazardous. The classical risk and reliability techniques are widely used to assess the system safety and performance. However, such techniques are less effective to quantify the system performance when system experiences dynamic changes due to component failures or configuration changes resulting from threats.

In order to achieve both safety and reliability in a balanced manner, systems must be designed with advanced concepts such as resilience features for enhanced performance without compromising the existing safety goals. Resilience is not an independent measure of safety from reliability and performance, instead it depends on such characteristics of the system. A reliable system can contribute to certain degree of safety and performance whereas a resilient system can exhibit robust safety and reliable performance. When a probabilistic model is available (i.e. known threats) reliability methods are proven approaches for the assessment of the system. However, when credible probabilistic models are not available or the primary cause of failures cannot be identified (i.e unknown threats), traditional reliability techniques are less reliable. The relationship between safety, reliability, performance and resilience is represented in Figure 1.

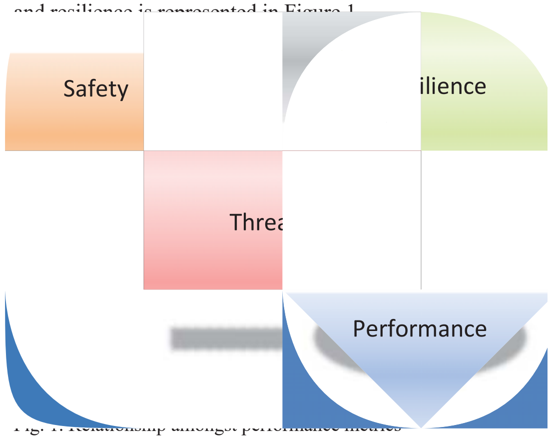

Fig. 1. Relationship amongst performance metrics

The resilience is directly contributing to both safety and performance whereas reliability is indirectly contributing to the overall system performance. This can be demonstrated with a conceptual calandria heat removal system shown in Figure 2. The system is designed to remove the heat generated in the calandria due to fission reaction in a typical nuclear reactor. The pumps take suction from the calandria and deliver back to the calandria through a set of heat exchangers and isolation valves. For the successful operation of the system, at least two out of three pumps and heat exchangers with associated valves in each closed working loop are needed to ensure continuous heat removal operation. The system failure not only reduces the availability of the reactor but also challenges its safety.

A threat is introduced on the pump circuit causing failure of one of the running pumps in any one working loop. As system now being operating with no redundancy, the system is expected to be restored within the stipulated time to avoid shutting down the reactor. Reliability of the system is usually evaluated over time by considering a fixed design configuration, however the resilience performance is evaluated over time with a specific configuration at time during disruption and recovery phase. Reliability doesn't consider the dynamic repair aspects unlike resilience which has significant effect on overall performance. The corresponding performance variation from a resilient design is shown in Figure 3. Here, the performance metric considered is the availability of the calandria heat removal system. The system shown in Figure 2 has several resilience performance states depending on the available resources and response time as shown in Figure 3. Whereas the same system has known reliability based on the working configuration over time. As the resilience strongly depends on many factors including human and organisational factors, the recovery time is proportional to the decision making and task execution. Hence, for the same threat could affect a change in both performance and recovery time. For example, performance 1, 2 and 3 indicate the system has encountered a minor performance loss due to failure of one of the running pumps but it was able to recover to normal performance state quickly after implementing necessary recovery actions within the stipulated time. Instead, performance state 4 shows that the calandria heat removal system lost its complete performance due to failure of more than one pump and entered into a failed state. The variation in performance levels is due to the uncertainty associated with individual components in the system.

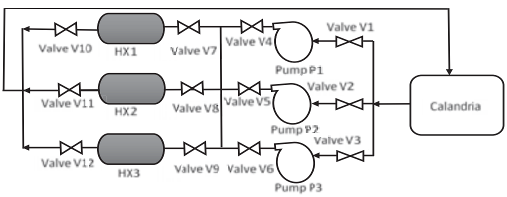

Fig. 2. Calandria heat removal system

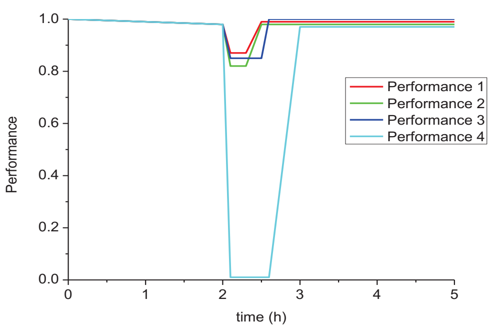

Fig. 3. Performance variation from a resilient system

2.1 *Resilience*

Resilience is an intrinsic capability and an inherent attribute of an engineering system. Resilience is also the capability of an entity to recover from an external disruptive event. Different definitions are proposed for different engineering systems depending on the parameter of interest. The effectiveness of a resilient critical infrastructure depends on its capability to anticipate, absorb, adapt, and rapidly recover from a disruptive event. Many researchers have proposed resilience definitions from different perspectives (see e.g. Woods, 2006; Youn et al., 2011; Min and Wang, 2015; Rundong, 2020). One widely known definition of resilience has been proposed by Cai et al. (2018) that defines resilience as the ability of an infrastructure to operate under anticipated or unanticipated threat scenarios after recovering from a sudden disturbance. Though, the resilience concept is popular in non-engineering fields, it remains a relatively new subject in the engineering domain and needs further research (Hosseini et al., 2016a). Hollnagel (2006) proposed a resilience framework which considers environmental, technical, social and economic aspects to deal with critical infrastructure safety. Since then, resilience engineering has gradually evolved as a potential alternative method to overcome the limitations of traditional risk assessment techniques (Steen and Aven, 2011) and various resilience metrics and their corresponding quantification methods have also been developed by various researchers.

Although various resilience metrics exist, quantifying the resilience for a specific engineering system remains a challenge because of internal and external factors involved in such metrics. Resilience is composed performance and time-dependent properties. System structure determines performance-based properties, such as robustness, adaptability, redundancy, flexibility, and survivability, whereas time-related properties, such as reparability, recoverability, rapidity, and resourcefulness are determined by maintenance resource. Hence, the structure of the system and maintenance resource are the key elements in determining overall resilience of the system.

2.2 *Resilience Quantification*

One of the major difficulty for quantifying resilience is the integration of organizational, human factors and social aspects with system structure (Chang and Shinozuka, 2004; Cimellaro et al., 2010). Despite the challenges, several researchers have successfully applied the resilience principles to assess critical infrastructure systems. Bruneau et al. (2003) proposed a conceptual seismic resilience framework based on complementary measures of resilience related to the probability of failure, consequences, and recovery time for civil infrastructure systems. Rocchetta et al. (2018) assessed the resilience of repairable power grids by subjecting to weather-induced failures with data deficiency. Santhosh and Patelli (2020) employed dynamic Bayesian networks to model the resilience of safety-related system of nuclear reactor incorporating the human and organizational factors. Estrada-Lugo et al. (2020) adopted Credal networks for estimating the resilience of primary system of a nuclear reactor in presence of lack of data and imprecision. Rundong (2020) reviewed metrics suitable for the resilience assessment of nuclear reactors and applied to an NPP considering two disruptive events, a small loss of coolant accident and station blackout. Cimellaro et al. (2010), in their approach, defined resilience quantitatively as the normalized area underneath a function Q(t) that governs the functionality of a system. Min et al. (2012) proposes a three-stage resilience analysis framework for urban infrastructure systems wherein authors apply a different strategy at each resilience stage during the threat phase. Francis et al. (2014) proposed a resilience metric that incorporates three resilience capabilities, including adaptive capacity, absorptive capacity, recoverability, and the time to recovery. Hosseini et al. (2016b) used static Bayesian networks to model infrastructure resilience and used a case of inland waterway port to demonstrate the method. The detailed discussion on quantitative resilience methods is beyond the scope of this paper. Readers are encouraged to refer to the cited articles. Although several quantitative methods are currently available, quantifying the resilience of a specific system remains a serious challenge.

2.3 *Factors Affecting System Restoration*

Resilience modelling involves identification of all possible recovery options for system to be able to respond to random disruptive events and recover the desired performance. The well implemented recovery actions may sometimes improve capabilities of the system relative to its normal operating condition (Tran et al., 2017). Such recovery actions include replacing or repairing of affected system or component and adapting a new operational strategy or reconfiguring an existing system. As most infrastructure systems require the involvement of human operators and strict adherence to organizational policies for repair or reconfiguration, and eventually restoration of the system, human and organizational factors play a key role in the recovery phase. The other important factors that affect the restoration efficiency are the maintenance related aspects, spare part availability, etc. which are well within the scope of the organization resource management and can be improved significantly subjected to safety, reliability and cost constraints. Human factors are highly complex to determine and may significantly change with respect to the type of disruptive event, and progressive scenarios of the random event (Kim et al., 2017, 2018).

2.4 *Modelling Human and Organisational Factors*

Performance assessment of human resources in most critical infrastructure is crucial and an important issue for managers, decision-makers and researchers. Amongst many factors, situation awareness and mental workload factors have the direct implication on the performance of human operator (Endsley, 1995; Fernandes et al., 2015; Seung et al., 2016). Situation awareness is related to perception of current state of the system, reasoning of the present state and projecting to an evolving state within the specified time and space (Hwang et al., 2008). It is more likely that an operator with good situation awareness skills is expected to assess the threat situation more accurately and take corrective actions more efficiently which greatly improves the resilience of the system. The other important factor is the physical and mental workload to assess the physical and mental needs of an operator during an emergency situation (Yang et al., 2012). Moreover, the performance shaping factors used to evaluate the operator's performance are strongly dependent on the potential consequences of the threats. Several researchers have proposed different techniques to model human and organisational factors in typical industrial problems (Endsley, 1995; Kim et al., 2017; Morais et al., 2020).

3 Methodology

System resilience is directly proportional to the successful recovery after the disruption. Recovery is not only related to the resources and actions but also include the functioning of the failed system which is reliability. Hence, recovery is a function of resources such as safety functions and their maintenance aspect, spare parts and the human actions involved in restoration. The framework also requires identification of potential recovery actions. These recovery actions enable a system to respond to random disruptions and recover the lost capabilities. Some recovery actions may even improve system capabilities relative to normal operating conditions.

Example recovery actions include repairing damaged systems and adapting or reconfiguring existing system structure. Typical recovery sequences exhibited from a resilient critical infrastructure upon a random disruptive event are shown in Figure 4. Depending upon the available recovery options the system may experience a partial or a complete loss of functionality as illustrated in Figure 4. The resilience profile for the minor loss sequence can be described as follows. From Figure 4, $\phi_n(t)$ represents the performance of the system corresponding to the initial stable state. The performance metric considered here is the availability of the critical system. After the occurrence of disruptive event at time t_e, the performance of the system degrades and converges to a disruptive state at time t_{d1} with performance value of $\phi_{d1}(t)$ corresponding to disruptive state. During time $t_{d1e} - t_{d1}$, the situation of the disruptive state of the system is assessed and necessary recovery actions are implemented at time td1e. After successful recovery, the system reaches a new performance state $\phi_{f1}(t)$ at time t_{r1} which is also a measure of the availability. The resilience of such a recovery sequence can be computed from the proposed models discussed in Section 2.2.

In this study, we employ the time-dependent model proposed by Henry et al. (2012) to quantify the resilience of system for a case of minor loss sequence and defined in following equation

$$\varphi_r(t) = \frac{\phi f1(t) - \phi d1(t)}{\phi n(t) - \phi d1(t)} \tag{1}$$

The resilience of each successful recovery sequence is evaluated using the above equation.

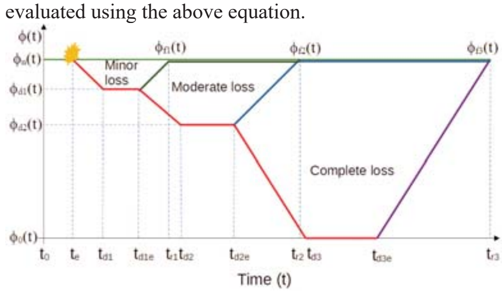

Fig. 4. Typical recovery sequences of a resilient critical infrastructure

When system is expected to have multiple recovery sequences the overall (net) resilience of a system may be computed by taking the geometric mean of all the recovery sequences with associated weightage for each successful recovery. Hence, the overall system resilience is termed as the net area under the multiple system response curves after a disruptive event. The net resilience can be defined as the effective resilience of a system obtained by combining all the possible successful recovery sequences in a response to the disruptive event. The overall resilience of a system with multiple recovery sequences is mathematically computed as in Eq. (2):

$$\Phi_R = [\prod_{r=1}^{n} w\varphi_r(t)]^{\frac{1}{n}} \quad (2)$$

where, $\varphi_r(t)$ is the resilience of each successful recovery sequence given by Eq. (1), r is the number of successful recovery sequences of a system after a disruptive event, w is the weight associated with a specific recovery sequence. Alternatively, resilience of any single sequence can also be computed from Eq. (1). For example, the resilience due to moderate loss according to Figure 4 can be computed from Eq. (3) and that due to complete performance loss can be computed from Eq. (4) as follows:

$$\phi(t) = \frac{\varphi_{f2}(t) - \varphi_{d2}(t)}{\varphi_n(t) - \varphi_{d2}(t)} \quad (3)$$

$$\phi(t) = \frac{\varphi_{f3}(t) - \varphi_{d3}(t)}{\varphi_n(t) - \varphi_{d3}(t)} \quad (4)$$

In addition, when the system is subjected to series of threats with corresponding recoveries, and the occurrence of each threat is independent of the other then the net resilience of the system is computed as a geometric mean value as shown in Eq. (5):

$$\Phi_{NR} = [\prod_{i=1}^{n} \Phi_{Ri}]^{\frac{1}{n}} \quad (5)$$

where n represents the number of threats on a system and Φ_{Ri} is the net resilience due to combination of disruptive event. Alternatively, the overall resilience may be computed by considering resilience response as analogous to a typical parallel system as given in Eq. (6):

$$\Phi_{NR} = 1 - \prod_{i=1}^{n}(1 - \Phi_{Ri}) \quad (6)$$

Resilience as such is not a direct metric of system performance, instead it is obtained from reliability or availability. In addition, there are no benchmark for resilience in the current literature (to the best of authors' knowledge) to compare specific analysis findings. However, a higher value towards 1.0 signifies system being more resilient as resilience is derived from classical performance metrics such as reliability of availability.

Based on the recovery features available within the system design such as automatic sensing and actuation, human intervention, etc. the weights may be assigned to each recovery sequence. Table 1 shows typical weightage factors for each successful recovery sequence in case of auto, manual or complete shutdown recovery for a typical threat on reactor regulation system. The weightage factors shown here are only for illustration, a more accurate factors may be assigned to each recovery sequence from the operational experience or from an expert elicitation.

The assignment of the weightage factors is based on the available design features to recover the system. For example, in auto setback recovery case it is apparent that the amount of effort required to restore the system is less in comparison with manual setback recovery where more human operator involvement is expected. Similarly, when system doesn't recover either by auto or manual setback it not only takes longer to recover but also require more effort to restore in terms of shutting down and identifying the restoration resources including safety systems. Since resilience is a property of both system as well as organisation, and strongly depends on restoration capability, any change in these aspects significantly affects the overall resilience. Hence, the weightage factors have significant role in determining the effective resilience of the system. In order to demonstrate the proposed framework on a typical industrial case study Petri net approach is employed in this study. A brief discussion on Petri nets is given in the next section.

Table 1: Weightage factors

Recovery	Weightage factor
Auto setback	0.99
Manual setback	0.89
With shutdown	0.79

3.1 *Petri Nets*

A Petri net is a graphical and mathematical tool for modelling and analysis of discrete event systems. Petri nets were conceived and described by Carl Adam Petri in his PhD thesis (Petri, 1962). They are widely used in many fields such as automation, control systems, communication, economy, reliability, and management. A Petri net is an oriented graph with two types of nodes called places (P) and transitions (T) as shown in Figure 5. The nodes are connected by oriented arcs. The arcs connect places to transitions and transitions to places. A place gives information about a local state and a transition represents an event that changes the state of a Petri net. A place is drawn as a circle and a transition is drawn as a bar or a rectangle. A place can represent, for example, required resources, input data, or input signals. A transition can be, for example, a task, computations, or signal processing. The number on arc represents the number of token required to fire a transition and a number of token to be delivered to a particular place as illustrated in Figure 5b and 5c. A thorough description on Petri nets can be found in Murata (1989).

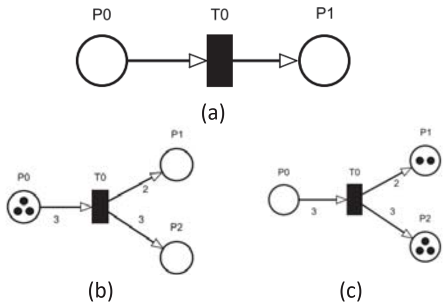

Fig. 5. Basic models of Petri net: (a) simple Petri net model, (b) Transition T0 enabled, (c) Transition T0 fired.

4. Resilience of Safety Related Nuclear System

The proposed method has been applied to a safety related reactor regulation system of advanced thermal nuclear reactor to assess its net resilience (Sinha, 2006). The main function of the regulation system is to regulate the control rods to maintain reactor under normal operating conditions. Threat on regulating system results into loss of regulation accident if not mitigated. This system consists of twelve control rods (four regulation rods, four shim rods and four absorber rods). Regulating rods are used for reactivity control operation, shim rods are used for reactor setback operation and absorber rods are used for xenon override.

The operation of these control rods is based on a 2-out-of-3 sensor logic. To demonstrate the application of proposed method to a critical infrastructure, Petri net technique is employed which models regulation system of nuclear reactor along with auto and manual setback recovery functions with a threat on control rods. Threat is simulated on one of the four absorber rods of a regulation function, and system response is studied by actuating auto/manual setback functions in response to disruption by propagating a token (i.e. absorber rod failure) over the Petri net model. Upon activation of threat by transition T0_Threat, and when transition T1_Rod_Fail fires, absorber rod is said to be failed which laces a token in place P2_Rod_Fail. Based on the transition probabilities associated with auto setback, manual setback and shutdown recovery, the failed system enters into one of these three states and recovers once restoration measures are implemented. Apart from various internal or external disturbances on system, human and organizational factors, crucial in achieving overall system resilience, are also modelled in the restoration phase as situation awareness and physical mental workload factors.

Depending on success/failure states of the control and shim rods, together with human and organizational resilience the system is restored to a new performance state. The temporal aspects of component states, and human and organizational factors are accounted via probability distributions in the Petri net model. Several threat scenarios are postulated based on the available safety and redundancy measures within the system to demonstrate various resilience sequences exhibited from the system. The threat scenario resulting into various resilience sequences is described below: One of the four control rods is affected by an internal threat causing complete failure of that control rod. Since the functioning of regulation system depends upon the successful operation of all the control rods, failure of one control rod initiates the auto or manual setback function 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 back to a normal working state. In the event of automatic setback being not actuated due to failure of sensing and switching circuit, the manual setback is initiated by the intervention of human operator. In the unlikely scenario of failure of both automatic and manual setback functions the mitigation and restoration are completely dependent upon the available safety systems and human intervention. Depending upon the resulting threat scenario the resilience sequence evolves accordingly. The failure and repair data for various components of regulation system is taken from generic data source IAEA Tecdoc 478 (1998) and the performance shaping factors required for assessing the situation awareness and mental workload are taken from NUREG/CR-6949 (2007). A simplified Petri net model of the regulation system with associated recovery functions is shown in Figure 6.

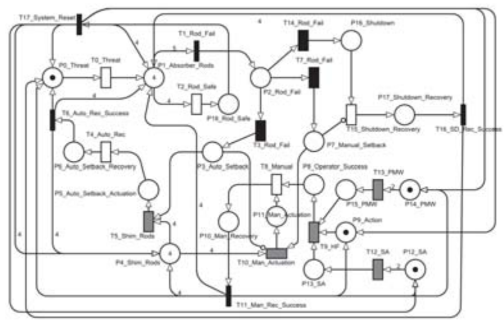

Fig. 6. Petri net model of regulation system of a nuclear power plant

The initial state of threat, control rod working, shim rods under standby and the human and organisational factor states are shown with a token in it. When a token reaches into a control rod place it signifies the threat has activated and it is likely that it will affect the control rods. When a transition T1 fires then the control function is said to be failed. Once the control rod failure is detected by the sensing and switching circuit a token is transferred to place P3 activate the auto setback function. In the event of failure auto setback, the manual setback is actuated by the intervention of human operator by placing a token in place P7. If both auto and manual setback functions fail, then a token will be placed in place P16 which activates the recovery after a complete shutdown. Upon successful recovery or if none of the control rods fail then the tokens will be reset to their initial states. The Petri net model shown in Figure 6 is simulated over a mean time of 2.9h starting from an initial steady state until complete recovery state after a disruptive event on regulating rods with 1million simulations to determine the recovery time and recovery probability of various sequences. The time 2.9h is determined from various transition probabilities associated with components and recovery actions. Since the control rod failure rate is of the order 10^{-5}, it was necessary to simulate at least 10^{6} simulations to observe control rod failure. The recovery sequences of auto and manual setback functions after the disruptive event for three simulation sequences are shown in Figure 7. Again, the performance metric shown is the availability of regulation function.

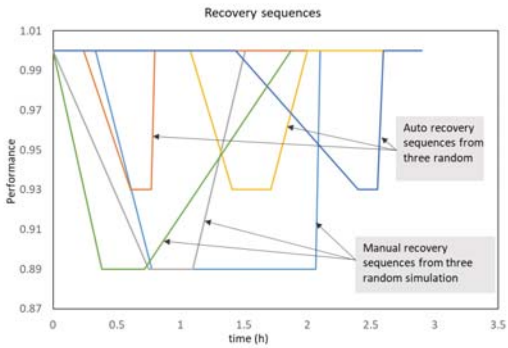

Fig. 7. Recovery sequences

It is observed from Figure 7 that several recovery sequences are possible for restoration of the affected system. Therefore, it is important to estimate the net resilience resulting from different recovery sequences. Due to the large number of simulations performed, it is practically impossible to manually identify each successful random recovery sequence and then compute the net resilience. However, this can be automated with suitable computer program. Therefore, the net resilience in this study is computed from only six successful recovery sequences. Santhosh and Patelli (2020) have performed the resilience assessment of same case study on regulation system using Bayesian approach and quantified the performance metric, which is availability for various states including steady state, disruptive and recovery states for various sequences. The recovery time information obtained from the simulated Petri net model and the performance of the recovered system obtained from Santhosh and Patelli (2020) are used to compute the net resilience metric. From Eq. (1), the resilience of each auto recovery sequence and manual recovery sequence are found to be 0.83 and 0.9 respectively. Taking into account the weightage factors as shown in Table 1, and from Eq. (2) and Eq. (5) the net resilience of regulation system is found to be 0.81. It may be noted that the performance of system after each recovery needs to be evaluated separately before evaluating the net resilience. For simplicity, we have used the same performance value for all the sequences of auto (0.93) and for manual (0.89) from Santhosh and Patelli (2020). Also, the resilience computed in this study is only for a single event, however the approach may be extended in case of multiple threat scenarios.

5. Conclusions

A quantitative resilience assessment framework for critical systems is proposed and applied to a regulation system of nuclear power plant. This approach presents a novel means to compute the net resilience by combining the possible recovery sequences either from a single disruptive event or from a series of threats and providing a single resilience metric of the critical infrastructure system.

The applicability of the proposed framework has been demonstrated by using a Petri net model of the regulation system. The probability of system being in various states when disruptive event occurs is estimated and the recovery time recorded. By using the weightage factors the net resilience of regulation system is computed for a single disruptive event. The proposed approach can be easily extended to compute the overall net resilience of a system resulting from a series of disruptive events over time.

It is important to evaluate the performance of system after each recovery and then compute the net resilience for each disruptive event before computing the overall effective resilience. It is worth noting that the weightage factors used in this study are only for illustration of the approach, a more accurate factors may be derived from the operational experience or from an expert elicitation for each recovery sequence based on the recovery features available within the system design such as automatic sensing and actuation, human intervention, etc. This new approach considers temporal aspects of the system together with human and organizational factors towards quantitative evaluation of system resilience over internal/external threats thus demonstrating its flexibility to be applicable to various critical infrastructure systems. However, when the system is very large and complex, there is a possibility of state-space explosion particularly when Petri net or Bayesian network are employed. The quantitative resilience metrics are new and help the industry and academia in setting the safety margins for their critical infrastructure systems considering all the possible recovery options.

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

Azadeh, A. 2016. An intelligent framework for productivity assessment and analysis of human resource from resilience engineering, motivational factors, HSE and ergonomics perspectives, Safety Science, 89, 55-71.

Bruneau, M., Chang, S.E., Eguchi, R.T., Lee, G.C., O' Rourke T.D., Reinhorn, A.M., et al. 2003. A framework to quantitatively assess and enhance the seismic resilience of communities. Earthq Spectra, 19(4):733–52.

Chang, S.E., Shinozuka, M. 2004. Measuring improvements in the disaster resilience of communities. Earthq Spectra, 20(3):739–55.

Cimellaro, Gian, P., Andrei, M. Reinhorn, Bruneau, M. 2010. Framework for analytical quantification of disaster resilience. Engineering Structures. 32, 3639–3649.

Endsley, Mica, R. 1995. Toward a theory of situation awareness in dynamic systems, Human Factors. 37(1), 32-64.

Estrada-Lugo, H.D., Santhosh, T.V., de Angelis, M., Patelli, E. 2020. An approach for resilience assessment of safety critical systems using Credal networks. Proceedings of the 30th ESREL and 15th PSAM Venice. https://www.rpsonline.com.sg/proceedings/esrel2020/pdf/4192.pdf

Fernandes Alexandra, Per Øivind Braarud. 2015. Exploring measures of workload, situation awareness, and task performance in the Main Control Room, Procedia Manufacturing. 3, 1281 – 1288.

Francis, R., B. Bekera. 2014. Application of Petri nets to reliability prediction of occupant safety systems with partial detection and repair. Reliab Eng Syst Saf 121, 90–103.

George-Williams, Hindolo, Min Lee, and Edoardo Patelli. 2018. Probabilistic Risk Assessment of Station Blackouts in Nuclear Power Plants. IEEE Transactions on Reliability 67 (2): 494–512. https://doi.org/10.1109/TR.2018.2824620.

Henry, D. and Ramirez-Marquez, J.E. 2012. Generic metrics and quantitative approaches for system resilience as a function of time. Reliab Eng Syst Saf 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).

Hosseini Seyedmohsen, Kash Barker, Jose E. Ramirez-Marquez. 2016a. A review of definitions and measures of system resilience, Reliab Eng Syst Saf. 145, 47–61.

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

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 SSG-3. 2010. Development and application of Level-1 Probabilistic Safety Assessment for Nuclear Power Plants.

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

Kim Yochan, Jinkyun Park, Wondea Jung. 2017. A classification scheme of erroneous behaviors for human error probability estimations based on simulator data, Reliab Eng Syst Saf. 163, 1–13.

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. Reliab Eng Syst Saf. 173, 12–22.

Lay, E., M. Branlat, Z. Woods. 2015. A practitioner's experiences operationalizing, resilience engineering. Reliab Eng Syst Saf. 141, 63–73.

Min Ouyang, Zhenghua Wang. 2015. Resilience assessment of interdependent infrastructure systems: With a focus on joint restoration modelling and analysis. Reliab Eng Syst Saf. 141, 74–82.

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

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.

Murata, T. 1989. Petri nets: properties, analysis and applications. Proc. IEEE 77, 541-580.

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.

Petri A. 1962. Kommunikation mit Automaten. PhD thesis, Institut fur Instrumentelle Mathematik, Schriften des IIM.

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, 339-350. https://doi.org/10.1016/j.apenergy.2017.10.126

Rundong, Y., Tolo, S., Dunnett, S., Andrews, J. and Patelli, E. 2020. Resilience in the Context of Nuclear Safety Engineering. In RAMS. https://nottinghamrepository.worktribe.com/OutputFile/4154117.

Santhosh, T. V., and Patelli, E. 2021. Resilience Engineering: Principles, Methods and Applications to Critical Infrastructure Systems, in Ehsan Noroozinejad Farsangi (ed.) Reliability-Based Analysis and Design of Structures and Infrastructure. 1st Edition, CRC Press/Taylor & Francis Publisher, ISBN 9780367758080.

Santhosh, T.V. and Patelli, E. 2020. A Bayesian network approach for the quantitative assessment of resilience of critical systems. Proceedings of the 30th ESREL and 15th PSAM Venice.https://www.rpsonline.com.sg/proceedings/esrel2020/pdf/3699.pdf

Seung, Woo Lee, Ar Ryum, Kim, Jinkyun, Park, Hyun, Gook Kang, and Poong Hyun Seong. 2016. Measuring Situation Awareness of Operating Team in Different Main Control Room Environments of Nuclear Power Plants, Nuclear Engineering and Technology. 48, 153-163.

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, Reliab Eng Syst Saf 119, 88–94.

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

Steen, R., and Aven, T. 2011. A risk perspective suitable for resilience engineering. Safety science, 49(2), 292-297.

Stellman, J.M. 1998. Encyclopaedia of Occupational Health and Safety. International Labour Organization.

Tran, H.T., Michael Balchanos, Jean Charles Domerçant, Dimitri N. Mavris. 2017. A framework for the quantitative assessment of performance-based system resilience. Reliab Eng Syst Saf. 158, 73–84.

Woods, D. D. 2015. Four concepts for resilience and the implications for the future of resilience engineering. Reliab Eng Syst Saf. 141, 5–9.

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.

Yang, Chih-Wei, Li-Chen Yang, Tsung-Chieh Cheng, Yung-Tsan Jou, Shian-Wei Chiou. 2012. Assessing mental workload and situation awareness in the evaluation of computerized procedures in the main control room, Nuclear Engineering and Design. 250, 713– 719.

Youn, B.D., Chao Hu, Pingfeng Wang. 2011. Resilience-Driven System Design of Complex Engineered Systems, Journal of Mechanical Design. October, 133 / 101011-1-15.

Zhao, Yunfei, Jiejuan Tong, Liguo Zhang, Guohua Wu. 2020. Diagnosis of operational failures and on-demand failures in nuclear power plants: An approach based on dynamic Bayesian networks, Annals of Nuclear Energy 138, 107-181.