Resilience in the context of Nuclear safety engineering

Rundong Yan, Loughborough University
Silvia Tolo, Nottingham University
Sarah Dunnett, Loughborough University
John Andrews, Nottingham University
Edoardo Patelli, Liverpool University

Key Words: Nuclear power, Resilience, Petri nets, Simulation, Natural hazards

SUMMARY & CONCLUSIONS

The safety and reliability of critical infrastructures is a key challenge in modern societies. This is all the more true when referring to the nuclear power industry, due to the rigid safety requirements on the one hand and the growing complexity of new systems on the other. The current study investigates the potential of a resilience engineering approach in dealing with current and future challenges in the context of nuclear reactor safety. The efficiency of several resilience metrics for capturing systems' performance in the case of accidents are discussed, and a novel framework for resilience analysis of nuclear reactor is proposed. The overall aim of this work is to provide computational and theoretical tools for resilience evaluation, paving the way for its application in the nuclear industry.

1 INTRODUCTION

With more than 400 nuclear reactors currently operating in the word and several decades of operational history, nuclear power generation is widely recognized to be a well-established and mature technology. However, due to the potentially catastrophic consequences of nuclear accidents, the safety of such facilities has consistently nurtured the concern of the public opinion as well as of the scientific community. Indeed, accidents such as those occurred at Three Mile Island, Chernobyl and Fukushima have highlighted the vulnerability of nuclear installations to a wide range of hazards, from human errors to natural disasters and design defects, and have demonstrate the potential safety issues associated with NPP's. This has inspired much research on risk assessment and safety design for nuclear systems. As a result, techniques such as Event tree analysis and Fault tree analysis have reliably supported the development of safe nuclear reactor designs for many years [1]. However, the introduction of novel and more complex reactor designs, involving an increasing use of automation and a wide digitization of control systems, while providing unquestionable advantages in terms of efficiency, has the potential to introduce new and often not fully understood vulnerabilities into the systems. This, alongside more strict safety standards and new emerging threats such as cyber-attacks and software bugs, has exacerbated the need for a step change in the safety philosophy employed.

The current research investigates the adoption of a resilience engineering approach as the key for the implementation of novel methodologies able to tackle all aspects of nuclear safety, from design and operation to accident response and recovery.

2 RESILIENCE ENGINEERING

Resilience Engineering is still in its early stages of development and its application in the nuclear industry is limited and not fully explored [2, 3]. Differently from conventional risk assessment methods, resilience approaches aim to bypass the resilience on historical information making space for proactive solutions aiming at anticipating and planning for the unexpected. However, resilience engineering is still far from being well established or widely applied, and even lacks a universally agreed definition. Most of the available definition of resilience incorporate four critical aspects: avoiding threats, withstanding threats, recovery from threats and adapting to threats [4]. It is common practice to visualize these features as a system resilience curve (SRC). As shown by the generic SRC provided in Figure 1 (adapted from [5]), the system operation is assumed to be characterized by a steady-state performance (Phase 1) until the occurrence of the disruptive event at time t_0. This compromises the normal operation of the system, triggering the action of available safety systems aimed at mitigating and absorbing the impact of the event during Phase 2. The worst state of the system, reached at time t_1, is expected to be restricted within the recoverable region before any recovery actions can be conducted. It is worth noting that the gradient of the curve and the value of the performance minimum reached within Phase 2 depend on many factors such as the magnitude of the event, the available safety systems, the response time of control systems, etc. In Phase 3, recovery actions are conducted to restore any critical functionality of the system. The duration of this phase depends strongly on the difficulty of identifying, diagnosing all failures and conducting the corresponding recovery actions. Following this, the system can be fully restored to its original status and restart its operation in Phase 5. However, as shown in Phase 6, the system

is expected to learn from the event occurred so to improve its resilience against future similar events.

Despite the large reference to SRC and the general enthusiasm surrounding the concept of resilience in almost all engineering fields, the available frameworks entailing this kind of analysis provide mostly vague guidelines and fail in offering a widely agreed upon metrics for system resilience. The proposed research aims at filling such gap, investigating suitable metrics for the resilience analysis of nuclear reactors. The candidate metrics have been compared based on their ability to capture the dynamic behavior of system's performance, and the four key elements of resilience previously discussed. For demonstration purposes, a CANada Deuterium Uranium (CANDU) reactor design and its response to several disruption event has been analyzed. Finally, the outline of a novel framework for resilience analysis of nuclear power reactors is proposed and briefly discussed.

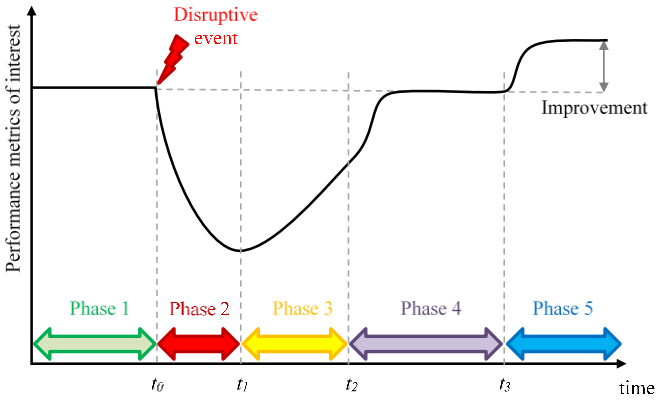

Figure 1. System resilience curve, representing normal operation (Phase 1), shock and response (Phase 2), recovery and maintenance (Phase 3), performance restoration (Phase 4), adaptation from threat (Phase 5)

3 CASE STUDY

The analysis carried out in this study considers the behavior of a typical CANDU reactor [6] subject to different accidents. Figure 2 shows the primary heat transport system of the reactor, where the uranium fuel is loaded into horizontal pressure tubes. The heavy water coolant is pumped through the reactor core's tubes in a closed loop ensuring the removal of heat produced by the fission chain reaction in the reactor. The available thermal power is then transferred to a secondary cooling loop in the form of high-pressure steam obtained with the use of steam generators. The steam powers the turbines resulting in the production of power by the electric generators.

3.1 Safety systems

The CANDU design includes a series of safety features aimed at enhancing the reactor's tolerance to accidents. Two independent and diverse, fast-acting safety shutdown systems are in place: the primary system relies on the use of neutron-absorbing shutoff rods suspended above the reactor by electromagnets; the secondary system is designed to inject high-pressure gadolinium nitrate into the moderator. However, the fuel inside the reactor will continue to produce decay heat after the reactor shutdown, hence requiring continuous cooling. All electrical instruments are powered by the offsite power supply. If this latter is lost, the electricity generated by the reactor onsite is used. As further mitigation strategy, there are three back-up diesel generators working as standby generators, while additional three emergency diesel generators are stored in a dry area, offsite or on high ground, in the case of failure of all other onsite and offsite power sources. The time required to start a standby or emergency generator is expected to be less than 5 minutes. Each diesel generator can provide enough power to ensure the circulation of cooling water to the steam generators. In the case of unavailability of all diesel generators, water can be fed to the steam generators by a gravity driven water system (GDWS) which is connected to a water storage tank. Furthermore, upon the failure of all the power sources, a battery group is in place to supply sufficient power for lighting and essential equipment such as monitoring systems for several hours but not for reactor cooling. In the case of a leak in the heat transport system, the emergency coolant injection system (ECIS) refills the heat transport system to ensure water continues to circulate. The very unlikely failure of all the mentioned safety systems would trigger the activation of further back-up emergency strategies, including three fire trucks that can pump coolant from local water sources into the calandria and a larger vessel containing heavy water acting purely as a moderator. The radioactive steam and water eventually leaked in the containment would be sucked into the vacuum building and cooled. It is worth mentioning that the vacuum building design is a unique safety feature of CANDU reactors.

3.2 Accident scenarios

All components and subsystems of a nuclear reactor are subject to possible failure due to natural decay. This can in turn lead to further failures and hence different accident scenarios.

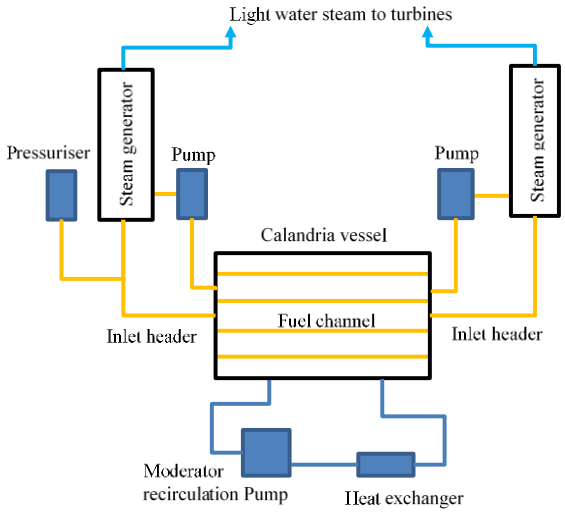

Figure 2. A schematic of a CANDU primary heat transport system (adapted from [7])

Two typical design accidents for nuclear reactors, namely loss of coolant accident (LOCA) and station blackout (SBO), are taken into account in this study.

A LOCA entails a break in the heat transport system [7]. It is usually classified according to the break size: a large break will lead to a rapid loss of coolant, so that the core temperature could increase dramatically. The fuel temperature might rise sufficiently high for the Zircaloy steam reaction or even reach the melting point of the reactor core within 5 seconds. The accident is characterized by a short power transient and then the shutdown system is activated automatically. Due to the break in the heat transport system, an alternative cooling system, known as the ECIS, will be activated to keep cooling and removing decay heat after the safe shutdown. If the ECIS fails as well, the fire trucks will be required to intervene. As discussed in the previous section, any leaked materials to the containment will be sucked away and cooled by the vacuum building to prevent containment rupture due to overpressure. In case of failure of all the cooling systems, the temperature of the fuel will keep increasing and eventually lead to a complete core melting, which can be considered as not recoverable. Indeed, a similar occurrence at the Three Mile Island accident in 1979 resulted in a cleanup effort lasting about 14 years. In contrast to this, a small break means a lower rate of loss of coolant, which may make the detection more difficult and hence could lead to a delayed response.

SBO is caused by the failure or cut off, of the offsite power supply. In the event of an SBO accident, the system itself is expected to produce enough electrical power onsite to continue the normal operation of the reactor avoiding a shutdown until the offsite power supply is recovered. However, if the onsite power supply fails to start, the shutdown system is activated automatically. After the shutdown of the reactor, the decay heat needs to be removed continuously by the natural circulation due to the complete loss of power. However, to ensure the availability of coolant, the steam generators have to be filled with cool water. This requires the correct operation of extraction pumps. As mentioned, the operation of just one back-up generator would provide the amount of power required for this process. If all back-up generators fail, the gravity driven water system (GDWS) is required to provide enough water in the steam generator to maintain the natural circulation, allowing time for the fire trucks to intervene.

4 PERFORMANCE METRICS

In the current study, resilience has been defined as 'the ability of assets, networks and systems to anticipate, absorb, adapt to or rapidly recover from a disruptive event'.

However, the resilience of systems cannot be measured directly, so that its assessment has to rely on the monitoring or analysis of third parameters and their transient in the case of abnormalities. In this study, five reactor critical parameters, namely core temperature, coolant pressure, containment pressure, power production and probability of core damage have been considered for the creation of resilience profiles in the case of small break LOCA (SBLOCA) and SBO. The choice of the first three parameters is justified by the advantages that directly measurable indicators would introduce in terms of ease of monitoring and their potential in highlighting safety issues. Besides its direct measurability, power production has been considered as a potential resilience indicator due to its obvious potential for representing the availability of the system. Differently from the other parameters investigated, the probability of core damage is a dimensionless, not directly measurable quantity that implies the use of mathematical models for its computation (e.g. relying on physical quantities such as temperature and availability of safety systems). However, this parameter has been included in the current study for the capability of quantifying the effectiveness of safety systems and mitigation measures as well as for continuity with the current probabilistic safety assessment (PSA) practice.

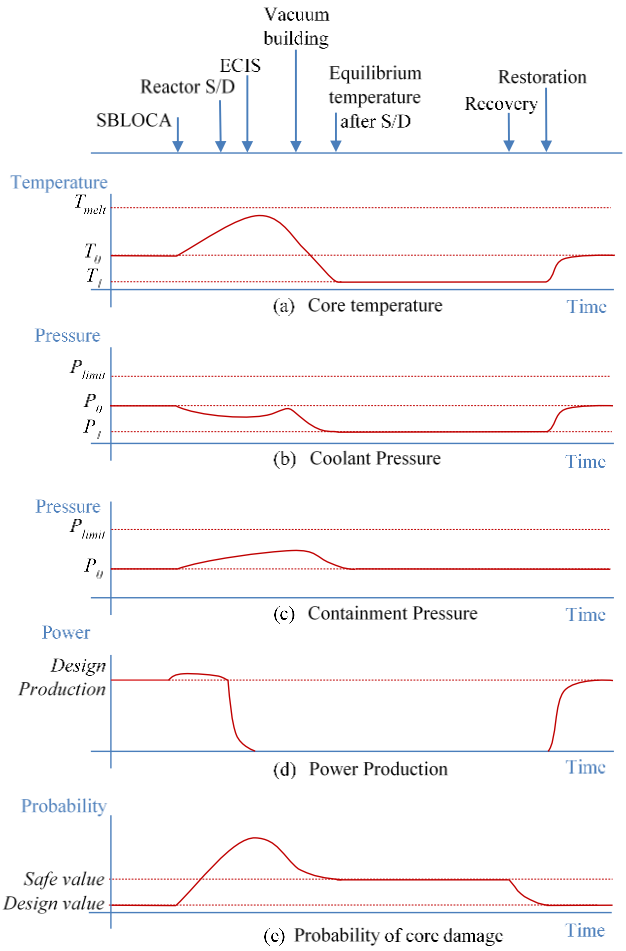

Figure 3. Parameter profiles after a SBLOCA (Scenario 1)

At this early research stage, the resilience profiles plotted for the parameters discussed have been deduced hypothetically for the purpose of identifying the most suitable metrics. Further research will focus on the systematic construction of the selected parameter profile using advanced physical model simulation methods. Two different scenarios are compared for each accident.

Scenario 1 for the SBLOCA case relies on the assumption that all the safety systems in place are operative. In this case,

shown in Figure 3, the occurrence of a SBLOCA is expected to:

- cause a progressive increase of the core temperature (Fig. 3(a)), triggering the automatic shut-down of the reactor and the activation of the ECIS. This would cause the temperature to decrease progressively until a new equilibrium is reached;
- trigger a gentle decrease of the coolant pressure (Fig. 3(b)), which could be balanced by the injection of coolant performed by the ECIS. Also, the accident would result in the definition of a new equilibrium, characterized by a lower coolant pressure due to the requirement of a smaller amount of water to cool the decay heat than that required during normal operation. On the other hand, the containment pressure increases due to the leaking from the break and then drop back to normal after the activation of the vacuum building, as shown in Figure 3(c);
- cause the interruption of power production due to the reactor shutdown (Figure 3(d));
- increase the probability of core damage (Figure 3(e)), which is assumed to be dependent on the core temperature as well as on the availability of mitigation systems.

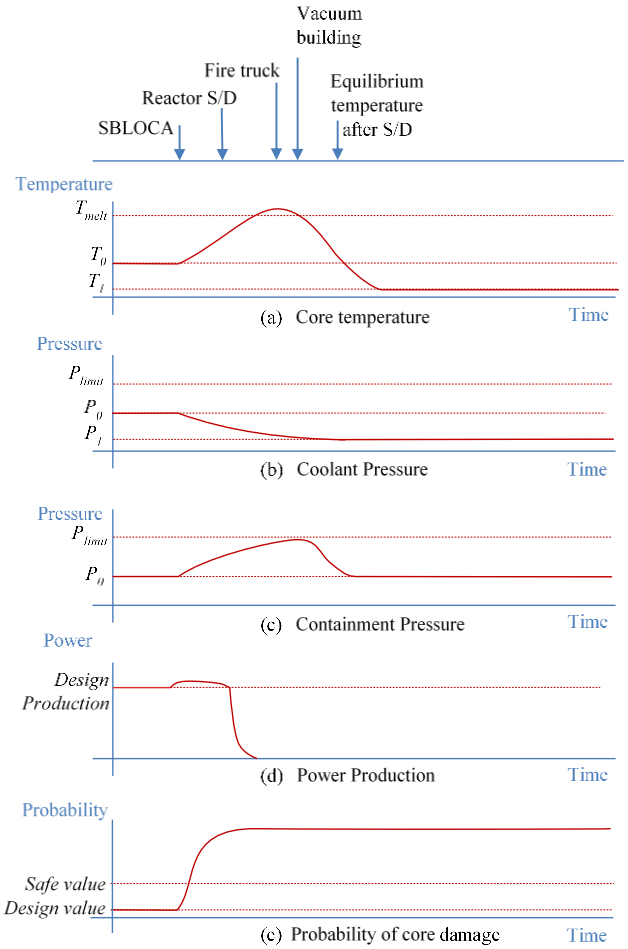

Figure 4. Parameter profiles after a SBLOCA (Scenario 2)

The operation of the reactor can be expected to be recovered within a given time since the damage is limited. The restoration of operation would finally bring all the reactor parameters back to their design value.

In the case of unavailability of some safety systems, the parameters evolution would significantly differ from the trends plotted in Figure 3. In the second scenario of the SBLOCA case, the ECIS is assumed to be unavailable, so that the fire trucks have to be used instead. The time required to put the trucks in place is much longer than that needed for the activation of the ECIS. Hence, the fuel will stay at a higher temperature for a longer period before cooling as shown in Figure 4(a). This implies the damage of the reactor core. The containment pressure could rise and approach to the critical rupture value as shown in Figure 4(c). The irrecoverability of the reactor is well captured by the trend of the probability of core damage, as shown in Figure 4(e). Once the core is damaged severely, it is not possible to predict the recovery time of the reactor due to the cleanup of radioactive materials and more importantly the unpredictability on a social scale.

With regards to the occurrence of an SBO, this would cause only a small increase in all the parameters profiles, as shown in Figure 5, since the reactor shutdown is not required and the onsite generation would supply the power necessary to the correct operation of the plant.

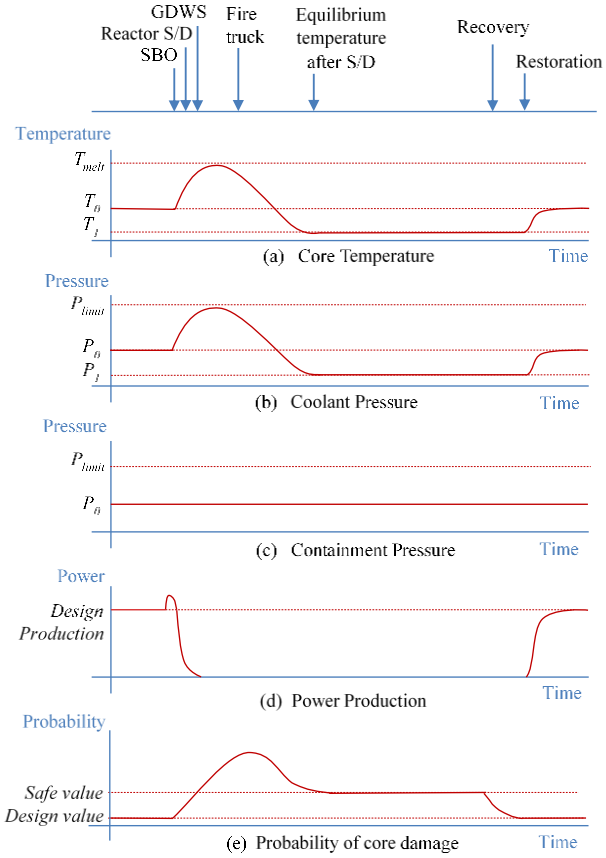

Figure 5 Parameter profiles after a SBO (Scenario 2)

Conversely, the scenario 2 of the SBO case, assumes the unavailability of onsite power and the failure of all back-up. This results in:

- the increase of core temperature triggering the reactor shutdown. The raise in core temperature is partly mitigated

by the action of the GDWS which ensure the availability of natural circulation until the intervention of fire trucks (see Figure 5(a)), avoiding core damage;
- a slight decrease of the coolant pressure (Figure 5(b)) while the containment pressure remains stable thanks to the lack of leakage (see Figure 5(c));
- the interruption of power production due to the reactor shutdown (see Figure 5(d));
- increase of the probability of core damage, which decreases after intervention of the available safety systems.

4.1 Comparison and Discussion

From the analysis carried out, the ability of physical, directly measurable quantities (such as process parameters and power output) to capture the resilience of the system appears to be strongly limited. For instance, estimating the resilience of the system based on the reactor power output allows capturing thoroughly any trend or change concerning the systems' availability over the ongoing accident interval. However, this is not matched by the capability of satisfactorily measuring and portraying the system safety. Indeed, the power production may be still ongoing even in the case of failure of minor subsystems or secondary safety systems, which instead would unquestionably lower the resilience (and safety) of the overall plant. Hence monitoring the power output does not provide sufficient information on the reactor safety and overall state. Since the safety of the reactor core is inextricably connected with the availability of cooling, process parameters such as coolant temperature and pressure may at first seem an obvious and reasonable choice for a resilience. Indeed, while failing to capture the availability of the system, they provide crucial information on the state (and safety) of the ongoing physical process: any external event able to affect significantly the primary cooling system, would indeed trigger the perturbation of the coolant flux. However, the suitability of such options for the assessment of systems resilience is hardly satisfactorily, mainly due to the locality of such measurements. As for the previous case, similar metrics are not able to depict changes that, although not directly affecting the physical process, have the potential to lower the ability of the system to absorb and safely respond to accidents, disruptive events or external hazards. In light of these considerations, the probability of core damage appears to be the most promising metric for resilience assessment among those considered. Although this still fails to include in the assessment the availability of the system, it provides a good understanding of the state, and in particular of the safety, of the overall system. It is opportune to stress that, in the absence of a metric able to track both system availability and safety during accidents, priority should be given to the second in the monitoring of nuclear systems, due to the high risks associated with the entailed physical processes. Moreover, from a purely conceptual point of view, the use of a dimensionless quantity to measure system resilience is highly preferable to the previous options considered. It must be clarified that the use of probability values in this context does not lead the analysis back to a mere system reliability calculation: the aim of the metrics is indeed to track the evolution of the system state along accident scenarios instead of providing a point estimate of its probability of failure.

5 METHODOLOGY AND FUTURE WORK

As discussed in the previous section, the analysis carried out suggests that the metrics based on the probability of core damage, although still affected by limitations (e.g. being strongly safety-focused), is the best available option for capturing the resilience of nuclear systems. However, it is worth highlighting that the efficiency of such assessment is only as good as the framework for the calculation of such metrics. Considering this, the core of future research will be the definition of a robust methodology and the implementation of accurate models for resilience assessment based on the probability of core damage. The approach currently under development relies on the implementation of a system model depicting accurately the complex network of dependencies existing among the nuclear reactor subsystems (including instrumentation and control systems) as well as their interaction with the ongoing physical processes entailed. To capture the entire range of technological and physical failure scenarios, the model under development consists of two main parts. The first is dedicated to reproducing the interaction among the different system's components, in order to fully portray the possible consequences of individual and common cause failures on the overall process and to study the eventual trigger and evolution of domino effect. The input for this section of the model entails physical quantities (e.g. reactivity of the reactor, temperature of the core etc.), while the main model parameters fall in the domain of technological failures and embrace single component failure rates as well as accident scenarios hypothesis (e.g. assuming the initial unavailability or degradation of certain components due to external hazards). Thanks to the capability to model asynchronous and concurrent processes and to analyze delays in timed systems, Petri Nets have been selected for modelling the reactor system architecture and characteristics. This part of the model is designed to provide in output the system's configuration (e.g. state of actuators, location of control rods etc.) as well as the state of process parameters directly affected by it (e.g. coolant pressure, temperature etc.). This information will be then fed to the second section of the model, dedicated to the analysis of the physical processes entailed by the reactor operation to calculate the reactivity of the reactor and the thermal power produced. This in turn will be submitted to the first part of the model as input (e.g. the updated value of core temperature), establishing a simulation cycle which will cover the entire time extent of the accident scenario under study. To sum up, for each accident scenario under consideration, the availability and state of each component is defined and the evolution of the scenario over time, in terms of system absorption, response and recovery, analyzed dynamically through the discussed coupled model.

Uncertainty will be taken into account characterizing stochastically the components failure rates and propagating measurements errors in the computation. The probability of core damage will be calculated comparing the simulated core temperature against a reference threshold selected according to

the characteristics of the physical system under study. The value of the probability obtained through the process described will refer to the specific case scenario assumed for the specific cycle of simulations. Hence, the resilience profile obtained tracking the evolution of the core damage probability along the time domain of the accident will refer to a specific scenario. It is worth highlighting that, regardless of the choice of resilience metrics, the approach described can be easily applied to different metrics and resilience definitions without further modifications. The methodology briefly introduced implies a significant computational burden: to guarantee the feasibility of the simulation, the model and its analysis will be implemented using the C++ language, in an object-oriented, parallel fashion.

6 CONCLUSIONS

In this paper, metrics suitable for the resilience assessment of nuclear reactors are investigated and discussed. This was achieved by studying the response of a traditional CANDU reactor design to two disruptive events, a small loss of coolant accident and station blackout. For each of these scenarios, two cases were analyzed, respectively assuming the availability and unavailability of safety systems. Based on the assumptions introduced, the profiles for several resilience metrics were built and compared in terms of their suitability for the overall assessment of the system. The analysis carried out suggests the probability of core damage as the most suitable metric to fully capture the complexity of the system and measure its resilience, although strongly safety-focused. Based on the results obtained, the paper outlines the computational framework for resilience assessment currently under development in the NuRes (A Resilience Modelling Framework for Improved Nuclear Safety) project. This would rely on the adoption of Petri nets for modelling the nuclear reactor system, and hence the interaction of its subsystems during accident scenarios, and for the construction of profiles capturing the system's performance in the case of disruption for resilience analysis purposes.

7 ACKNOWLEDGEMENT

The authors would like to acknowledge the financial support of EPSRC through grant EP/R021759/1, part of the UK-India Civil Nuclear Collaboration program

REFERENCES

1. N. C. Rasmussen, *Reactor Safety Study –An Assessment of Accident Risks in US Commercial Nuclear Power Plants, WASH-1400*, US Nuclear Regulatory Commission, Washington, DC,1975.
2. J. Park, T. P. Seager, P. S. C. Rao, M. Convertino, I. Linkov, "Integrating Risk and Resilience Approaches to Catastrophe Management in Engineering Systems," *Risk Analysis*, Vol. 33, No. 3, (Mar.) 2013, pp 356-367.
3. J. T. Kim, J. Park, J. Kim, P. H. Seong, "Development of a quantitative resilience model for nuclear power plants," *Ann. Nucl. Energy*, Vol 122, (Dec.) 2018, pp 175-184.
4. S. Hosseini, K. Barker, J. E. Ramirez-Marquez, "A review of definitions and measures of system resilience," *Reliab. Eng. & Syst. Safety*, Vol 145, (Jan.) 2016, pp 47-61.
5. S. R. Greene, "Are Current U.S. Nuclear Power Plant Grid Resilience Assets?", *Nucl. Technol.*, Vol. 202, 2018, 1-14.
6. CANDU 6 Program Team, "CANDU® 6 Technical Summary", Reactor Development Business Unit, 2005.
7. NUCLEAR ENERGY AGENCY, *Nuclear Fuel Behaviour in Loss-of-coolant Accident Conditions*, Report, 2009

BIOGRAPHIES

Rundong Yan MEng
Department of Aeronautical and Automotive Engineering
Loughborough University
Loughborough, Leicestershire, LE11 3TU, UK

e-mail: R.Yan@lboro.ac.uk

Rundong (Derek) is a Research Associate at Loughborough University, UK. He is in the final stage of his PhD where the focus of the research is analysing the reliability of automated guided vehicles.

Silvia Tolo, PhD
Faculty of Engineering
University of Nottingham
Nottingham, NG7 2RD, UK

e-mail: silvia.tolo@nottingham.ac.uk

Silvia is a Research Associate at Nottingham University, UK. She received her PhD from Liverpool University UK.

Sarah Dunnett, PhD
Department of Aeronautical and Automotive Engineering
Loughborough University
Loughborough, Leicestershire LE11 3TU UK

e-mail: s.j.dunnett@lboro.ac.uk

Sarah is a senior lecturer at Loughborough University, UK and a member of the Control and Reliability Research Group.

John Andrews, PhD
Faculty of Engineering
University of Nottingham
Nottingham, NG7 2RD, UK

e-mail: john.andrews@nottingham.ac.uk

John is Head of the Resilience Engineering Research Group at the University of Nottingham, UK.

Edoardo Patelli, PhD
Institute for Risk and Uncertainty
University of Liverpool
Liverpool, L69 7ZX, UK

e-mail: edoardo.patelli@liverpool.ac.uk

Edoardo is a Senior Lecturer at Institute for Risk and Uncertainty,

University of Liverpool, UK.