Proceedings of the 32nd European Safety and Reliability Conference (ESREL 2022)
Edited by Maria Chiara Leva, Edoardo Patelli, Luca Podofillini, and Simon Wilson
©2022 ESREL2022 Organizers. *Published by* Research Publishing, Singapore.
doi: 10.3850/978-981-18-5183-4_S24-06-676-cd

A Methodology for the Dynamic Risk Assessment of Nuclear Batteries

Federico Antonello

Department of Nuclear Science and Engineering, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139, USA. E-mail: afederic@mit.edu; federico.antonello@polimi.it

Jacopo Buongiorno

Department of Nuclear Science and Engineering, Massachusetts Institute of Technology (MIT), Cambridge, MA 02139, USA. E-mail: jacopo@mit.edu

Enrico Zio

Energy Department, Politecnico di Milano, Via La Masa 34, 20156 Milan, Italy and also with the Mines ParisTech, PSL Université Paris, Centre de Recherche sur les Risques et les Crises, 06904 Sophie Antipolis. *E-mail: enrico.zio@polimi.it*

Nuclear Batteries (NBs) are a unique class of nuclear micro-reactors, which are gaining attention for their potential to be a transportable, flexible, affordable, and decentralized low-carbon power source. The commercialization and efficiency of NBs require dedicated advanced risk assessments to address potential hazards, threats, and vulnerabilities that may challenge both safety and security. This work performs the advanced safety assessment of the nuclear battery designed at MIT, making use of a novel methodology that integrates *i*) System-Theoretic Accident Model and Processes (STAMP) principles to guide a qualitative exploration of the threats of the novel design, *ii*) Best Estimate Plus Uncertainty (BEPU) framework to investigate the behavior of NBs under accidental scenarios, and *iii*) the Goal-Tree Success-Tree Master Logic Diagram (GTST-MLD) framework to assess risk quantitatively. The integration of STAMP, BEPU and GTST-MLD provides systematic risk insights, giving due account to the NB interactions and dependencies among systems, structures and components.

Keywords: *Dynamic Risk Assessment, STAMP, STPA, Goal Tree Success Tree - Master Logic Diagram, Best Estimate Plus Uncertainty, Nuclear Battery, Nuclear Micro Reactors.*

1. Introduction

Nuclear Batteries (NBs) are standardized plug-and-play micro-reactors that generate 1 to 20 MW of heat and/or electricity, providing low-carbon energy for various applications, such as chemical processes, manufacturing, desalinition of water, hydrogen, food production, ship propulsion, to mention a few. They are envisioned as reliable, resilient and autonomously operating installations requiring minimal maintenance. They can deliver electricity, heat, and clean water to rural, maritime and military locations, where it is impervious to supply energy by traditional nuclear reactors, thermal power plants and renewable sources (Buongiorno et al., 2021). Kilopower (Gibson et al., 2017) of National Aeronautics and Space Administration (NASA), Megapower (McClure et al., 2015) of Los Alamos National Laboratory (LANL) and eVinci micro-reactor (Levinsky et al., 2018) of Westinghouse are examples of reactor designs for nuclear batteries. Their licensing and commercialization require dedicated advanced risk assessments to identify and effectively address potential hazards, threats and vulnerabilities that may challenge safety and security. However, NBs are relatively novel designs that remain largely untested and lack failure data and past information. Therefore, the traditional Probabilistic Risk Assessment (PRA) framework, which stands on knowledge and information on past failures, is not apt to describe the dynamic behavior of the novel NB designs, identify unknown threats and hazards, and assess the risk.

This work performs the advanced safety assessment of the nuclear battery designed at MIT by making use of a novel methodology that integrates *i*) System-Theoretic Accident Model and Processes (STAMP) (Leveson, 2012) to guide a qualitative exploration of the NB threats and

hazards, *ii*) Best Estimate Plus Uncertainty (BEPU) framework to investigate the NB dynamic behavior during accidental scenarios, and *iii*) the Goal-Tree Success-Tree Master Logic Diagram (GTST-MLD) framework (Hu & Modarres, 1999) to assess risk quantitatively. The methodology provides systematic risk insights without the need to rely on knowledge and information from the past and enables a dynamic assessment of the risk profile. Moreover, the methodology is apt to investigate novel designs and identify unknown threats and hazards.

The remainder of the paper is organized as follows: Section 2 describes the NB designed at MIT. In Section 3, the methodology is described. Section 4 presents the results and findings of the performed safety assessment. Section 5 draws some conclusions and describes potential future lines of work.

2. The MIT Nuclear Battery Design

The NB design considered here is a 5 MW (thermal) high-temperature heat pipe reactor designed at MIT. The core is made of solid monolithic blocks of graphite with three types of channels that accommodate fuel, neutron moderators and heat pipes. Figure 1 shows the core cross-section and the hexagonal pitch of the Fuel Assemblies (FAs). Each FA comprises one large-size heat pipe, six fuel elements, six moderator elements made of yttrium hydride and six small heat pipes. The graphite blocks in the center of the core are unfuelled to provide large thermal inertia during accidental scenarios. A thick radial neutron reflector surrounds the core; Control Drums (CDs), encapsulated in the reflector, provide long-term reactivity control, whereas shutdown Control Rods (CRs) provide rapid reactivity control. Core and reflector are located in a canister which is itself encapsulated in a Reactor Vessel Auxiliary Cooling System (RVACS) for decay-heat removal via natural circulation. During NB normal operation, heat is transferred through the heat pipes to the heat exchanger and, then, to a secondary side Power Conversion Unit (PCU). The use of heat pipes eliminates the need for mechanical pumps, valves and large-diameter primary loop piping. Finally, there is a remote operator whose sole function is to monitor operations and actuate a manual SCRAM system, should the protection system fail to do so.

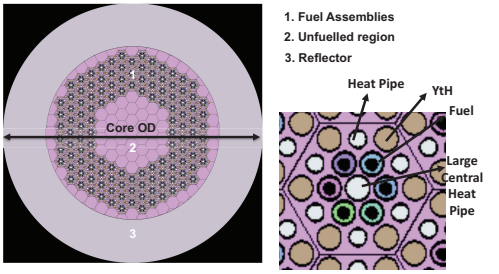

Fig. 1. Core cross-section and hexagonal pitch of the FAs.

3. The Proposed Framework for the Advanced Risk Assessment of NBs

The workflow of the proposed framework can be summarized in the following steps: 1) definition of the purpose of the analysis and the system goals; 2) representation of the NB elements, interactions, and dependencies by means of STPA control structures modeling and GTST-MLD (Hu & Modarres, 1999); 3) development of the M&S tools; 4) dynamic and quantitative risk assessment.

3.1. Purpose of the analysis and system goals

The first phase of the framework considers the STPA method proposed in (Leveson, 2012) in order to identify system boundaries, unacceptable losses, system-level hazards, and related system-level constraints. The collected information is used to construct the Goal Tree (GT) of the GTST-MLD by determining the goals of the analysis and the functions and subfunctions needed to achieve them.

3.2. SSCs elements and interactions representation

In the second step of the methodology, the STPA control structure model is developed to allow the reconstruction of the functional relationships and interactions supporting the operation of the NB (Leveson, 2012). The functions and subfunctions of the GT are used to identify the system processes, the controllers and their hierarchy. Then, each controller is associated with a set of control actions and feedbacks, which highlight how each subsystem and process is controlled and how it controls other subsystems and processes. As shown in Figure 2, each controller comprises *i*) a process model, which elaborates the feedback or signals from other controllers and/or processes, and *ii*) a control algorithm, which, based on the system state, actuates the control action.

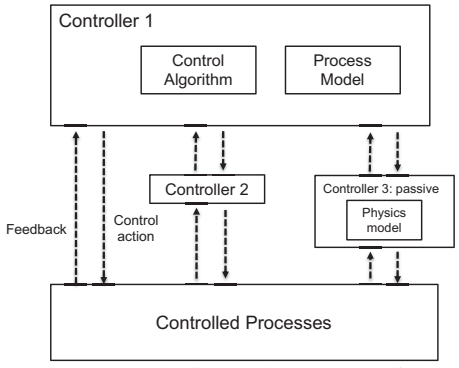

Fig. 2. An example of control structure modeling.

Then, STPA framework is considered to identify the Unsafe Control Actions (UCAs), which are the control actions that, in a particular context and worst-case environment, will lead to hazards. The NB interactions and dependencies are identified by analyzing the context and the mechanisms in which the controllers (and the corresponding SSCs) influence the processes and other controllers. Eventually, the influences among the physical elements and the IFs are highlighted in the MLD.

3.3. Development of the BEPU tools

The BEPU tools are developed to mimic the behavior of the NB during operation and accidental scenarios and to investigate the effects of IFs and relevant parameters on the simulation results. This step requires defining *i*) the input parameters for the simulation models, *ii*) their nominal values and uncertainty and *iii*) the simulation output, which are the parameters linked with the system-level constraints and limits. The BEPU also includes UQ and SA tasks. Given the computational burden required to run the tens of thousands of simulations needed to perform such tasks, we develop a surrogate model to speed up the simulation time of the simulation model. This step requires *i*) identifying the range of variation of the design and modeling parameters, and the associated probability distributions; *ii*) sampling various sets of input parameters with an ad-hoc sampling strategy, *iii*) performing the simulations considering the sampled input parameters and collecting the outcomes, and *iv*) training the surrogate models to learn, replicate and generalize the input-output relation. The surrogate model used in this work is the Gaussian Processes (GP).

3.4. Quantitative and Dynamic Risk Assessment

In this work, we use the surrogate models for *i*) performing the UQ and SA tasks, *ii*) computing the system failure probabilities with respect to the variation of the most critical parameters, and *iii*) quantifying the interactions and the combined effects of the most relevant parameters. Finally, the methodology provides a dynamic assessment of the risk profile.

3.4.1. Uncertainty Quantification

The UQ is performed by quantifying the probability distributions of the safety-relevant paraments associated with the identified safety limits (e.g., the Peak Cladding Temperature (PCT) during a transient). They are estimated by applying the surrogate model to 100,000 sets of input parameters sampled from the corresponding probability distributions.

3.4.2. Safety Margin

The safety margin $M(y_i)$, is here computed as the difference between the safety upper limit U_i and the value of a specific γ_1 percentile of the probabolity distribution of the safety parameter y_i, which by regulation is usually set equal to the 95-th percentile of the distribution of y_i and considers the uncertainties that affect y_i (Di Maio et al., 2016). The safety margin is computed as follows:

$$M(y_i) = \begin{cases} \dfrac{U_i - y_{\gamma_1}}{U_i - y_{i\,ref}} & if\ U_i > y_{\gamma_1} \\ 0 & if\ U_i \le y_{\gamma_1} \\ 1 & if\ y_{i\,ref} \le y_{\gamma_1} \end{cases} \quad (1)$$

where $y_{i\,ref}$ is a reference value, which in this work is the value of y_i when the input parameters are set equal to their nominal values.

3.4.3. Sensitivity Analysis

The sensitivity analysis is performed considering the Sobol main effect sensitivity index and the Sobol total effect sensitivity index (Saltelli et al., 2008).

3.4.4. Probability of exceeding the safety threshold and parameters interactions

The probability to exceed the safety limit due to the influence of the parameter X_i is here evaluated considering following procedure:

1. Set the value of the parameter $X_i = x'_i$
2. Sample N=10,000 sets of input parameters, changing all the parameters except $X_i = x'_i$
3. Perform the UQ and evaluate the probability of exceeding the limit given $X_i = x'_i$
4. Repeat 2 and 3 for different values of X_i to reconstruct the function f_i, which describes the variation of the probability of exceeding the safety limit with respect to variations of the variable X_i.

3.4.5. Dynamic Risk Assessment

In proposed methodology enables a dynamic risk assessment. In this respect, when time-dependent events occur, the time-dependent relationships and dependencies are modeled by considering the time as an additional input parameter for the metamodel.

4. Application to the MIT nuclear battery

This Section reports the results of the application of the proposed methodology to the safety assessment of the NB designed at MIT.

4.1. NB safety goals and purpose of the analysis

The STPA analysis identifies the environmental contamination as the reference loss. The associated hazard and system-level constraint are the release of radionuclides into the environment and that the NB must retain radionuclides, respectively. The reference goal for the GT is radionuclide retention, which needs the following main functions: *i*) NB integrity to avoid possible environmental contamination, *ii*) heat removal from the NB to avoid reaching excessive temperatures that can lead to component stress and failures, and *iii*) the NB criticality control, to avoid the occurrence of unexpected transients causing thermal and mechanical stresses. The GT functions are, then, used to identify the STPA system-level hazards and constraints. The GT and the step 1 of STPA are refined by repeating the process. This results in the identification of the specific constraints and limits, such as the cladding and moderator temperature limits, which are essential to achieve the main goal. In this work, we set the Peak Cladding Temperature (PCT) limit and the moderator temperature limit equal to 1804 K and 1373 K, respectively (Parisi et al., 2020; Wysocki et al., 2020).

4.1.2. NB modeling

For the sake of simplicity and to reduce the number the scenarios to be considered, in this work, we proceed assuming the occurrence of the unprotected Loss of Heat Sink (LOHS) event. This causes the sudden inability of the NB to exchange heat with the secondary side PCU and the malfunction of the mechanical reactivity control systems (e.g., the CDs and CRs). The reactivity is controlled only by the Reactivity Feedback (RF), whereas the heat is transferred radially through the core and the reflector and removed by RVACS.

Figure 3 shows the control structure model given the LOHS. The heat is generated in the fuel and, then, removed throughout cladding, graphite, reflector and canister to the RVACS. Each NB element is a passive controller acting to transfer heat from the hierarchically lower element. The mechanism is driven by the components temperatures, thermal properties, gap conductance among the elements, etc. The fuel temperature also depends on the power generated, which is controlled by the reactivity. The latter is driven by the RF that are influenced by the NB state (e.g., fuel temperature, moderator temperature, etc.).

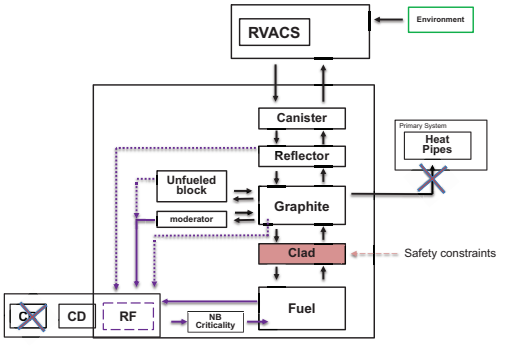

Fig. 3. Control structure of the NB, given the unprotected LOHS.

Figure 4 shows the part of the ST associated with the radial heat transfer and the developed MLD, which represents the influences and dependencies among the IFs, the relevant parameters and the SSCs of the NB. In this step, the IFs and parameters are also subdivided into controlling parameters (colored rectangles in Figure 4) and controlled parameters (dotted rectangles in Figure 4). The former are the design parameters that control the behavior of the NB during the

operation and accidental scenarios, whereas the latter are parameters associated with system-level constraints and limits.

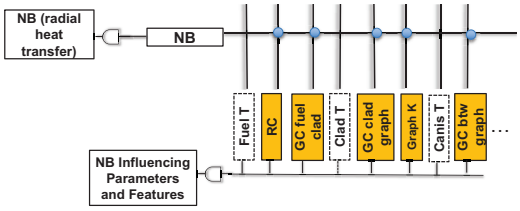

Fig. 4. Example of NB ST and the developed MLD.

4.3.1. NB simulation model

The NB simulation model has been developed using RELAP-5 3D code (Mesina, 2016). Table 4 gives the complete list of the input parameters. It includes the reactor power, the reactivity feedback coefficients, the gap conductance among the elements of the NB, the RVACS flow area, input air temperature and wall roughness.

Table 1. Simulation model input parameters and ranges of variation.

Parameter	Nominal Value [Range] [Distribution]
NB Power	5 MW [∓15%] [Uniform]
Reactivity Feedback Coefficients	Fuel Coef.: -1.5 pcm/K Range: [∓30%] [Uniform]
Graphite thermal conductivity	Temperature dependent function [∓10%] [Uniform]
Gap conductance in the core	10^4 W/m2-K [5×10^3-10^5] [LogUniform]
Gap conductance between canister and reflector	70 W/m^2-K [40-120] [Uniform]
RVACS flow area	0.3 m [0.2-0.4] [Uniform]
RVACS input air temperature	300 K [270-320] [Uniform]
RVACS wall roughness	10^{-4} [10^{-3}-10^5] [LogUniform]

The scenario is simulated through the following phases: 1) an initial period of normal operation of 100 seconds, 2) the sudden loss of heat transfer from the heat pipes to the heat sink and 3) the simulation of the following transient for 10,000 seconds.

4.3. Nuclear Battery Risk Assessment

The safety assessment includes: *i*) the UQ to identify the probability distribution of the PCT and the maximum moderator temperature under the LOHS accidental scenario, *ii*) the SA to identify the most relevant parameters and *iii*) the evaluation of the system failure probabilities, with respect to the variation of the most important parameters. Moreover, the obtained outcomes are also used to quantify the interactions and the combined effects of the most relevant parameters.

4.3.1. Uncertainty Quantification

Figure 5 shows the probability density of the PCT, the 95-th percentile, and the corresponding safety limit. Notice that the difference between the values of the PCT and the safety limit is large and assures a large safety margin. Figure 6 shows the probability distribution of the maximum moderator temperature, the 95-th percentile and the corresponding safety limit.

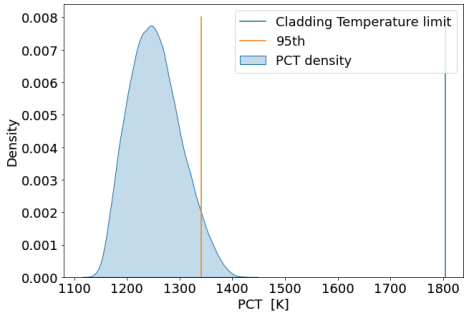

Fig. 5. PCT probability density, 95-th percentile, and corresponding safety limit.

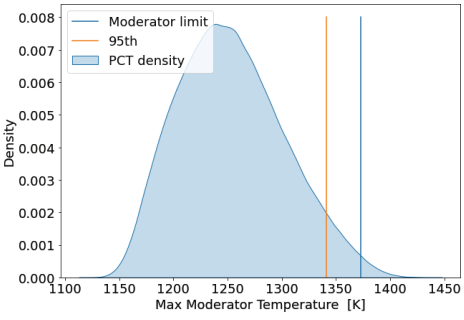

Fig. 6. Moderator temperature probability density, 95-th percentile, and corresponding safety limit.

The safety margins for the PCT and the maximum moderator temperature in our case are 0.87 and 0.32, respectively. Notice that, the safety margin for the moderator temperature is smaller than the one for the PCT, and may deserve additional analysis and consideration.

4.3.2. Sensitivity Analysis

The SA has been performed using the Sobol indices computed for the PCT and the maximum moderator temperature. The main contributors to the variance are the reactivity feedback

coefficient and the initial power. The contribution of the other parameters is negligible.

4.3.3. Probability of exceeding the safety threshold

Given the results obtained by the uncertainty quantification and the sensitivity analysis, the procedure of Section 3.4.4. is applied only to the maximum moderator temperature, and the considered parameters are the initial power and the reactivity feedback coefficients. Figure 7 shows the function f_i describing the probability of exceeding the limit for the two parameters. Notice that for reactivity feedback coefficients larger than 80% of the design values, the probability of exceeding the limit is 0, whereas, for lower values, the lower the coefficients, the larger the probability of exceeding the limit. Similarly, the f_i is larger than 0 only when the initial power is larger than 5.2 MW, which is 104% of the reference power. This analysis highlights critical ranges of values of the input parameters and provides insights useful to inform the STPA and reconstruct the loss scenarios and their causes.

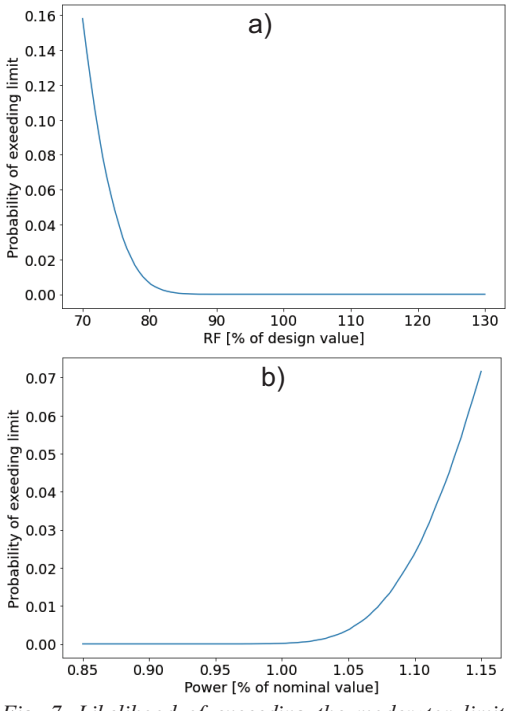

Fig. 7. Likelihood of exceeding the moderator limit given the value of the RF coefficient (7-a) and power (7-b).

4.3.4. Parameters interaction

The contribution of the combined effect of the two parameters with respect to their isolated effect is evaluated by performing the UQ considering the following four parameter ranges for initial power and reactivity feedback coefficients values: *a*) initial power larger than 104% and reactivity feedback coefficients lower than 80%, *b*) initial power lower than 104% and reactivity feedback coefficients lower than 80%, *c*) initial power larger than 104% and reactivity feedback coefficients larger than 80%, and *d*) initial power lower than 104% and reactivity feedback coefficients larger than 80%. Notice that, the likelihood of exceeding the safety limit for the ranges *b*), c) and *d*) is negligible, whereas it is equal to 0.104 for case a). Figure 8 shows the probability density function of the maximum moderator temperature, the 95-th percentile and the corresponding safety limit when the initial power and reactivity feedback coefficients are in the ranges of case a). The comparison with Figure 5 shows the relevance of the combined effect of the initial power and the reactivity feedback coefficients shifts the 95-th percentile of the temperature to exceed the safety limit. This results from the initial power and reactivity feedback coefficients being in the ranges of case a), whose probability is 0.061.

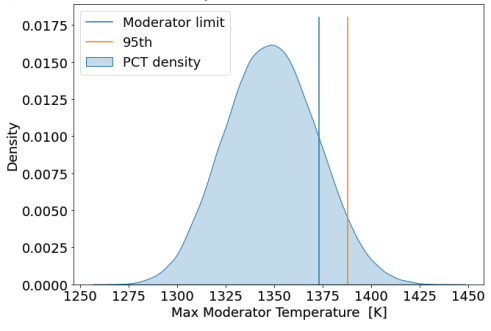

Fig. 8. The probability density function of the moderator temperature, the 95-th percentile and the corresponding safety limit when the initial power and RF coefficients are in the ranges of case a).

4.4. Dynamic Risk Assessment

To give an example of the ability of the proposed framework to enable a dynamic risk assessment, we consider the LOHS with a delayed actuation of the shutdown system. In this accidental scenario, the automatic shutdown system initially fails to detect the accident or actuate CRs and

CDs, and the reactor is shut down by the remote control monitor within 100 s.

Figure 9-a shows the variations of the 95-th percentile of the moderator temperature with respect to the time delay. As expected, the larger the delay, the larger the 95-th percentile of the moderator temperature, which is always well below the limit.

The dynamic response of the nuclear battery during the LOHS event in correspondence of the delayed activation of the shutdown system also influences the safety margins. Figure 9-b displays the dynamic characterization of the safety margins for the moderator temperature, when the reference value $y_{i\,ref}$ corresponds to the transient simulated by considering the input parameters equal to their nominal values, and the time delay equals to 1s, which is associated to the normal functioning of the shutdown system. Notice that, similarly to the 95-th percentile of the PCT of Figure 9-a, the larger the time delay, the lower the safety margin.

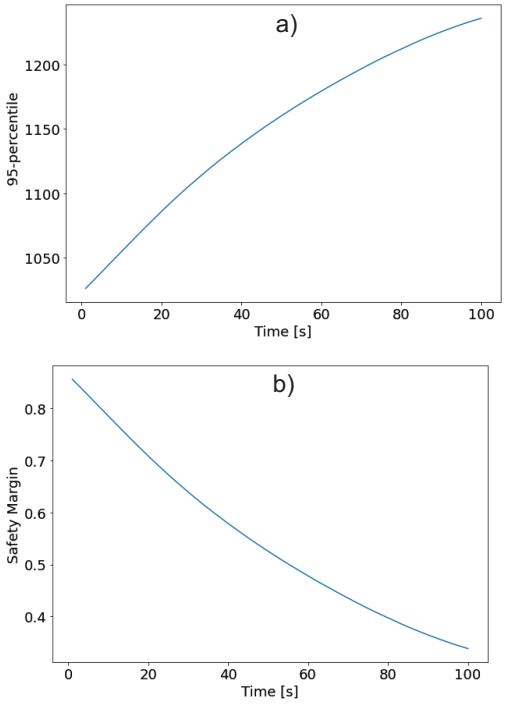

Fig. 9. 95-th percentile of the moderator temperature as a function of the time delay (9-a) and the corresponding dynamic characterization of the safety margins (9-b).

Figure 10 displays the variation of the main effect sensitivity index with respect to the time delay for the initial power, gap conductance between the canister and the reflector, air temperature, and reactivity feedback coefficients. It is worth underling that if the CRs are actuated within 1s from the beginning of the transient, the most influencing parameters are *i*) the initial power, *ii*) the gap conductance between the canister and the reflector, which influences the power extracted by the RVACS and the temperature difference between the core and the heat removal system, and *iii*) the RVACS inlet air temperature, which acts on the RVACS capability of removing heat. When the SCRAM is activated within a few seconds, the influence of the reactivity feedback coefficients is negligible. On the other hand, if the actuation of the shutdown system is delayed, the larger the delay the larger the importance of the reactivity feedback, which becomes predominant at 100 s. This shows the relevance of the time delay and the importance of performing dynamic analysis to reconstruct the scenarios and understand the phenomena involved. Finally, notice the capability of the NB in self-regulating after an accident, thanks to reactivity feedbacks which are able to substitute the shutdown system.

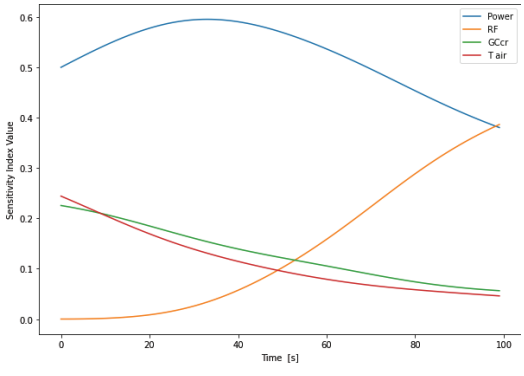

Fig. 10. Variation of Sobol main effect sensitivity index with time, for the initial power, gap conductance between the canister and the reflector, air temperature, and reactivity feedback coefficients.

5. CONCLUSION

This work presents the safety assessment of the NB designed at MIT using a novel framework that combines STAMP and STPA, BEPU and GTST-MLD. The results have shown framework capabilities to: *a*) identify the NB hazards, and the corresponding safety constraints and limits; *b)* highlight the most important components, features and parameters; *c*) drive the development of the (RELAP) simulation model; *d*) evaluate the

probabilities of exceeding the safety limits during accidental scenarios and identify the parameters contributing the most to it; *e*) estimate hidden unsafe parameters ranges and interactions; f) provide the dynamic assessment of the risk profile during accidental scenarios. Moreover, the analyses have shown the outstanding safety features of the NB, which is able to safely withstand the occurrence of an unprotected LOHS with large margins.

For future work, a research direction is to apply the proposed framework for a detailed and complete risk assessment of the NB. This is expected to confirm the capability of the framework to provide a dynamic risk profile during various accidental scenarios and to provide insights useful for the design and commercialization of the NB.

References

Buongiorno, J., Carmichael, B., Dunkin, B., Parsons, J., & Smit, D. (2021). Can Nuclear Batteries Be Economically Competitive in Large Markets? *Energies*, *14*(14), 4385. https://doi.org/10.3390/en14144385

Di Maio, F., Rai, A., & Zio, E. (2016). A dynamic probabilistic safety margin characterization approach in support of Integrated Deterministic and Probabilistic Safety Analysis. *Reliability Engineering and System Safety*, *145*, 9–18. https://doi.org/10.1016/j.ress.2015.08.016

Gibson, M. A., Oleson, S. R., Poston, D. I., & McClure, P. (2017). NASA's Kilopower reactor development and the path to higher power missions. *IEEE Aerospace Conference Proceedings*, *2017-June*, 1–14. https://doi.org/10.1109/AERO.2017.7943946

Hu, Y. S., & Modarres, M. (1999). Evaluating system behavior through Dynamic Master Logic Diagram (DMLD) modeling. *Reliability Engineering and System Safety*, *64*(2), 241–269. https://doi.org/10.1016/S0951-8320(98)00066-0

Leveson, N. G. (2012). Engineering a Safer World. In *Engineering a Safer World*. https://doi.org/10.7551/mitpress/8179.001.0001

Levinsky, A., Van Wyk, J., Arafat, Y., & Smith, M. C. (2018). Westinghouse eVinci Reactor for Off-Grid Markets. *American Nuclear Society Winter Meeting*, 11–15.

McClure, P., Poston, D., Rao, D., & Reid, R. (2015). *Design Of Megawatt P Ower Level Heat Pipe Reactors Los Alamos National Laboratory*. *November*.

Mesina, G. L. (2016). A History of RELAP Computer Codes. *Nuclear Science and Engineering*, *182*(1), v–ix. https://doi.org/10.13182/nse16-a38253

Parisi, C., Ma, Z., Mandelli, D., Anderson, N., & Zhang, H. (2020). Risk-Informed Safety Analysis for Accident Tolerant Fuels. *Nuclear Science and Engineering*, *194*(8–9), 748–770. https://doi.org/10.1080/00295639.2020.1732699

Wysocki, A. J., Jain, P. K., & Rader, J. D. (2020). *Transformational Challenge Reactor Accident Analysis* (2020 ANS Winter Meeting and Nuclear Technology (ed.); pp. 1–4). District of Columbia, United States of America.