Proceedings of the 33rd European Safety and Reliability Conference (ESREL 2023)
Edited by Mário P. Brito, Terje Aven, Piero Baraldi, Marko Čepin and Enrico Zio
 Published by Research Publishing, Singapore.
doi: 10.3850/978-981-18-8071-1_P684-cd

An Importance Function to Generate Scenarios for Training a Grey-Box Model for the Computational Risk Assessment of Cyber-Physical Systems

Juan-Pablo Futalef
Energy Department, Politecnico di Milano, Italy. E-mail: juanpablo.futalef@polimi.it

Francesco Di Maio
Energy Department, Politecnico di Milano, Italy. E-mail: francesco.dimaio@polimi.it

Enrico Zio
Centre de Recherche sur les Risques et les Crises, MINES Paris PSL, France.
E-mail: enrico.zio@mines-paristech.fr
Energy Department, Politecnico di Milano, Italia.
E-mail: enrico.zio@polimi.it

The operation, control and maintenance of many systems rely on the signal communication functions provided by telecommunication systems. This generates Cyber-Physical Systems (CPSs). Computational risk assessment is being advocated to properly account for the complexities and interdependencies of CPSs. However, simulation times can be high for practical feasibility. Surrogate models are being explored to address computational issues. Among these, Grey-Box Models (GBMs) have recently been proposed to merge the physical knowledge embedded into a high fidelity White-Box Model (WBM) with the learned-by-data knowledge used to train a Black-Box Model (BBM). In this paper, we propose the use of a novel Importance Function (IF) within a Repetitive Simulation Trials After Reaching Thresholds (RESTART) approach to simulate accidental scenarios for training BBMs, ultimately embedded into a GBM. A case study is considered concerning an Integrated-Power and Telecommunication (IP&TLC) CPS of literature.

Keywords: Cyber-physical system (CPS), Risk assessment, Rare events simulation, Black-box modelling, Grey-box modelling

1. Introduction

Cyber-Physical Systems (CPSs) integrate cyber and physical networks of components to enhance the performance of critical lifelines, such as energy, transportation, and communication (Cassottana et al. 2023; Zio 2018). Traditional risk assessment methods are unsuitable to tackle the heterogeneous complex dynamics and the numerous uncertainties characterizing the CPS components and their dependent behaviors (Cassottana et al. 2023).

Computational risk assessment can be used to explore CPSs responses in a multitude of scenarios (Di Maio and Zio 2017). Scenario generation amounts to simulating CPS responses to external stimuli (e.g., environmental factors and/or components operational conditions) and disruptive events (e.g., cyber-attacks and/or physical failures) that might occur. Post-processing allows discovering scenarios that might be overlooked by expert judgment or traditional risk assessment methods, and identifying causes and criticalities of the CPS.

Monte Carlo Simulation (MCS) (Zio 2013) is a straightforward way to generate scenarios, driven by the stochastic occurrence of discrete events. However, the number of scenarios to be simulated for exploring CPSs response is enormous, particularly when the significant scenarios have a small probability of occurrence (Di Maio and Zio, 2017). In practice, MCS is most of the times infeasible due to the computational burden related to running a high-fidelity White-Box Model (WBM) for the CPS response. Metamodeling by data-driven Black-Box Models (BBMs) can lower the computational demand while keeping a sufficient level of accuracy if enough data are available for training, yet they lack interpretation

(Peherstorfer, Willcox, and Gunzburger 2018). In-between WBMs and BBMs, Grey-Box Models (GBMs) are an attractive solution to reduce the computational cost of MCS, while preserving the fidelity and interpretability of the simulation outcomes. A sufficient number of scenarios that catch the CPS responses under normal and accidental conditions are needed to effectively train the BBMs embedded in the MCS (Futalef, Di Maio, and Zio 2022).

Rare events simulation methods can be devised to explore relevant scenarios. To name a few, we mention *splitting* (e.g., subset simulation (Cadini et al. 2012) and RESTART (Turati, Pedroni, and Zio 2016)), *Importance Sampling* (IS) (e.g., classical IS (Kroese, Taimre, and Botev 2011) and cross-entropy (Ansari, Chung, and Zio 2021)), and *Line Sampling* (LS) (e.g., traditional LS and variants (Dang et al. 2023)) methods. Splitting methods are suitable for CPS as they are designed for analyzing non-linear dynamical systems and are not strongly influenced by the dimensionality of the space of the model variables. RESTART can be particularly efficient since it avoids simulating uninteresting trials. Key tasks are defining the scalar mapping and the levels that drive the splitting.

In this work, we tailor RESTART to the problem of exploring CPS accidental scenarios for identifying the relevant ones for training the BBM of a GBM. For this, we propose a novel dynamic Importance Function (IF) that quantifies the vulnerability of the CPS along the simulated scenarios by accounting simultaneously for 1) the centrality of the CPS components exposed to hazards/threats and 2) the time-dependent susceptibility to failure of the CPS components. As we shall show, this allows RESTART to allocate computational time to simulate significant scenarios. Centrality metrics have been used for the reliability assessment of complex systems thanks to their capability of highlighting important components in terms of topology (Eusgeld et al. 2009; Devineni et al. 2020; Piccinelli et al. 2017). The selected centrality metric, i.e., the Current-Flow Betweenness Centrality (CF-BC) (Newman 2005) is static and ranks the components with respect to their topological relevance in fulfilling the system function.

Susceptibility, instead, dynamically quantifies the stress on a component throughout the scenario evolution, aiming at quantifying to which extent the component is endangered when exposed to some hazard(s). RESTART, guided by the novel IF, can guide the development of relevant accidental scenarios in which susceptible components (i.e., that bear at the same time the largest centrality and susceptibility along the simulation) can be damaged.

As a case study, we consider an Integrated-Power and Telecommunication (IP&TLC) CPS infrastructure of literature (Di Maio, Stincardini, and Zio 2022), that consists of a power grid equipped with a variety of cyber control units that communicate over a Telecommunication Network (TLCN). The results of RESTART guided by the novel IF are compared to those found when other IFs based on vulnerability metrics of literature (Di Maio, Stincardini, and Zio 2022) are adopted. Results show that the proposed IF outperforms the others in terms of relevant scenarios exploration.

The remainder of the paper is as follows. Section 2 recalls the RESTART method and presents the novel IF. Section 3 presents the case study and the comparison of different IFs. Finally, in Section 4 some conclusions are drawn.

2. CPSs Scenario Generation using RESTART

2.1. *Repetitive Simulation Trials After Reaching Thresholds (RESTART)*

RESTART is a rare events simulation method that proceeds as follows (J. Villén-Altamirano 2014; M. Villén-Altamirano and Villén-Altamirano 2011):

1) Let $\mathbf{x}(t) \in \Omega \subseteq \mathbb{R}^{n_x}$ be the state of a multi-dimensional stochastic process at time t with initial condition $\mathbf{x}(0) = \mathbf{x}_0$.

2) Let $\{\phi(\mathbf{x}(t)),\ t \geq 0\}$ be a scalar map $\phi: \Omega \rightarrow [0, \infty)$, called *Importance Function* (IF), whose domain is divided into m regions defined by the thresholds $T_i \geq 0$, $i \in \{1, \dots, m\}$, such that $T_{i'} > T_i$, if and only if $i' > i$. The regions $C_i := \{\mathbf{x} \in \Omega | \phi(\mathbf{x}) \geq T_i\}$ are nested (i.e., $\Omega = C_0 \supset C_1 \dots \supset C_m = A$), defining the intermediate regions $\Delta C_i := C_i - C_{i-1}$.

3) Run a *main trial*, which is a crude MCS of $\mathbf{x}(t)$, track $\phi(\mathbf{x}(t))$ and record the time(s) it up-crosses the threshold T_1; label the up-crossing event(s) as U_1 and the occurrence time(s) as t_{U_1}, saving the corresponding state(s) $\mathbf{x}(t_{U_1})$.

4) Perform $R_1 - 1$, $R_1 \in \mathbb{N}$, simulations called *retrials*, each of them starting from $\mathbf{x}(t_{U_1})$ and finishing at some end-of-simulation condition (e.g., mission time, occurrence of a fixed number of events, etc.) or when $\phi(\mathbf{x}(t))$ down-crosses T_1.

5) If during any of the R_1 retrials $\phi(\mathbf{x}(t))$ up-crosses the threshold $T_2 > T_1$, steps 2) and 3) are repeated, times t_{U_2} and states $\mathbf{x}(t_{U_2})$ saved and $R_2 - 1$, $R_2 \in \mathbb{N}$, new retrials simulated until the end-of-simulation condition or when T_2 is down-crossed.

6) Repeat steps 2) to 5) for all remaining thresholds and retrials, or until an end-of-simulation condition is reached, i.e., simulate $R_i - 1$ new retrials, $R_i \in \mathbb{N}$, when $\phi(\mathbf{x}(t))$ up-crosses any threshold T_i.

The rationale of RESTART is that it is more likely for $\mathbf{x}(t)$ to reach an intermediate region if it comes from an immediate lower-importance region rather than jumping, suddenly, across several. Therefore, simulating behaviors in higher-importance regions is favored, resulting in the allocation of more computational effort to the occurrence of low probability events that would be overlooked and the corresponding scenarios not used for training otherwise the CPS GBM.

2.2. *The Novel Importance Function*

In (Turati, Pedroni, and Zio (2016)), the cut sets of the system are obtained from its structure function and used to inform guide RESTART; however, cut sets identification in large CPS is impractical (Di Maio, Pettorossi, and Zio 2023). Then, typical CPS vulnerability metrics, such as Energy Not Supplied (ENS) or Power Generation Mismatch (PGM) (Di Maio, Stincardini, and Zio 2022), could be an alternative to guide the scenario generation; however, as we shall show in what follows, these yield unfruitful scenarios exploration for most of the computational time. To overcome the above limitations, we propose to combine a metric of the centrality of CPS components, typically used for network topology analysis, with a metric of their susceptibility, obtaining a dynamic metric that is used as IF to drive RESTART towards relevant scenarios of operational conditions.

As centrality metric, we adopt the Current Flow Betweenness Centrality (CF-BC) (Newman 2005), which ranks the importance of a component (electrical device/TLC gateway) based on the average topology-induced flow passing through it (electrical current/information). Let $G = (N, E)$ be a CPS graph, with N the n_N nodes (e.g., single-purpose components) and E the n_E edges (e.g., interconnections). Given sets of sources $S \subseteq N$ and targets $T \subseteq N$, the CF-BC of a j-th node is (Newman 2005):

$$c_j := \frac{\sum_{\{s<t\}} I_j^{(s-t)}}{(1/2)n_N(n_N - 1)}, \tag{1}$$

where $I_j^{(s-t)}$ is the flow due to a source-target pair of components $s - t$, $s \in S$ and $t \in T$. Notice that this metric provides a ranking of the components that is source/target dependent: by choosing the $s - t$ pairs, we can tune the exploration, focusing on the accidental scenarios affecting certain components instead of the entire network.

During the scenario evolution, the susceptibility of a component dynamically quantifies its usage level (or vice versa its resourcefulness) with respect to its factory ratings (i.e., the stress), when exposed to some hazard(s). Thus, susceptibility equal to zero means "no usage" (i.e., resourceful component), whereas susceptibility equal to one means "full usage" or "down" (resourceless component). Susceptibility $v_j(t)$ of a j-th component is:

$$v_j(t) := \begin{cases} \dfrac{\mathbf{x}_j^{(l)}(t)}{x_j^{+(l)}} & \text{if } j \text{ is operating;} \\ 1 & \text{otherwise,} \end{cases} \tag{2}$$

where $\mathbf{x}_j^{(l)}(t)$ is the l-th variable of the j-th component of the state vector $\mathbf{x}(t)$ and x_j^+ is its maximum allowed value that cannot be exceeded.

By coupling the centrality of Eq. (1) and the susceptibility of Eq. (2), we obtain the dynamic vulnerability metric:

$$\mathbb{v}_j(t) := c_j \cdot v_j(t). \tag{3}$$

The rationale is that $\mathbb{v}_j(t)$ emphasizes the role of components that contribute more to the vulnerability of the system when they are susceptible (almost to exceed the $x_j^{+(l)}$). The $\phi(\mathbf{x}(t))$ is thus set equal to the network-level vulnerability metric is defined as:

$$\phi(\mathbf{x}(t)) \coloneqq \mathbb{V}(t) \coloneqq \sum_{j\in\{1,\dots,n_N+n_E\}} c_j \cdot v_j(t) = \sum_{j\in\{1,\dots,n_N+n_E\}} \mathbb{v}_j(t) \qquad (4)$$

In practice, the network vulnerability $\mathbb{V}(t)$ of the CPS can be obtained by:

1) modeling the CPS by means of the state vector $\mathbf{x}(t)$ and the dynamics (i.e., the transition functions among the states of $\mathbf{x}(t)$);

2) mapping the CPS into a graph $G = (N, E)$, where nodes N are bar buses, generators, electrical loads, TLC gateways, controller units, and so on, and the edges E are transmission lines, transformers, fiber-optic cable, and so on;

3) calculating the CF-BC for all the elements in G. The sources S are generators and the control center, whereas targets T are customers and control units, defining the $(s-t)$ pairs;

4) computing, during simulation, the network-level vulnerability of each component $j \in N \cup E$ via Eq. (4).

2.3. *Performance metric*

To evaluate the performance of the proposed IF in guiding RESTART, we calculate ξ that accounts for the simulation effort allocated to reach a generic importance region ΔC, i.e., up-crossing the corresponding threshold T:

$$\xi(T) = \frac{\sum_t [\phi(\mathbf{x}(t)) > T]}{n_{\text{sim}}}, \qquad (5)$$

where the Iverson bracket $[\cdot]$ counts one when the condition is true or zero otherwise, and n_{sim} is the number of calls to the one-step state-transition function of $\mathbf{x}(t)$ along all the simulation runs (i.e., the total number of simulated points).

3. Case Study

The case study is an IP&TLC CPS that integrates an IEEE14 power grid including users and generators, a TLC network, and various control units (Di Maio, Stincardini, and Zio 2022). The Control Center (CC) collects the power load demands from the users and performs AC Optimal Power Flow (OPF) calculations. Since the OPF returns steady-state solutions, the model is discrete-time, where time $t_k = k\Delta t$, with $\Delta t > 0$ the (fixed) simulation time step and $k \in \{0,1,\dots\}$. Generators and customers are denoted $\mathcal{G}$ and $\mathcal{C}$, respectively; synchronous condensers are modelled as PV generators (thus, they belong to $\mathcal{G}$) with $0[MW]$ of both minimum and maximum active power limits. For simplicity, but without loss of generality, we assume the TLC to be perfectly working and always available for the dispatchment.

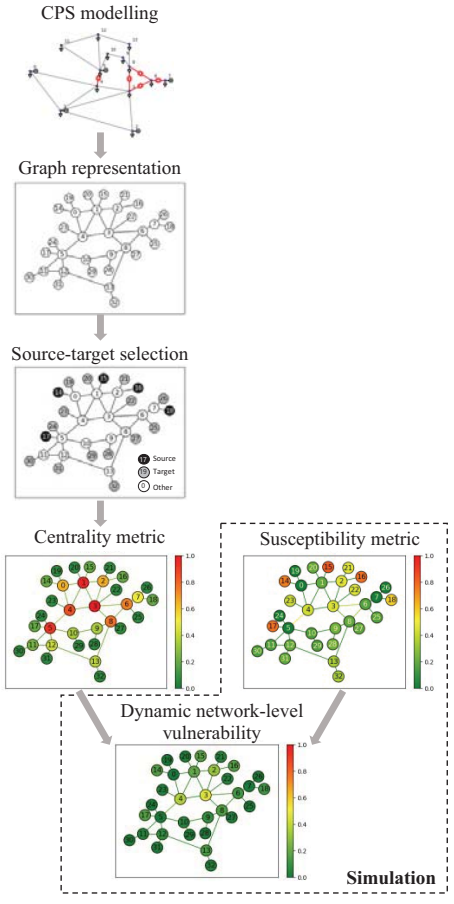

Figure 2.1 Steps for the calculation of the network-level vulnerability.

The IP&TLC CPS reacts to the external stimulus, denoted by $\mathbf{u}^{\mathrm{T}}(t) = [\mathbf{p}_d^{\mathrm{T}}(t), \mathbf{q}_d^{\mathrm{T}}(t)]$, where $\mathbf{p}_d(t)$ and $\mathbf{q}_d(t)$ contain the active and reactive power demands of each customer at time t, respectively. Their values are taken from (Di Maio, Stincardini, and Zio 2022), using 30 days of historical open data sampled every 15 minutes, made available by TERNA (Terna 2023). For generalization purposes, we process the TERNA data by applying min-max normalization and, then, multiply the results by the nominal active and reactive

Table 1 Repairment and failure rates of components

Component	λ_{Rep} $[h^{-1}]$	λ_{Fail} $[h^{-1}]$
Generator	24	3e-3
Transmission Line	12	3.5e-3
Transformer	4	19e-3

power load demands of each customer in the IEEE14 case.

The rest of the dynamic power grid variables are vectors containing the variables of the corresponding bus: $\mathbf{p}_g(t)$ and $\mathbf{q}_g(t)$ are the active and reactive power generations, $\mathbf{v}_m(t)$ and $\mathbf{v}_a(t)$ are the voltage magnitudes and angles, and $\boldsymbol{\pi}_{\mathbf{Gen}}(t)$, $\boldsymbol{\pi}_{\mathbf{Line}}(t)$, and $\boldsymbol{\pi}_{\mathbf{Trafo}}(t)$ are the binary components states, active (1) or down (0) for generators, transmission lines and transformers, respectively. Then, to track all the relevant variables, we define the IP&TLC state vector $\mathbf{x}(t)$ as:

$$\boldsymbol{x}(t) = \begin{pmatrix} \mathbf{p}_d(t) \\ \mathbf{q}_d(t) \\ \mathbf{p}_g(t) \\ \mathbf{q}_g(t) \\ \mathbf{v}_m(t) \\ \mathbf{v}_a(t) \\ \boldsymbol{\pi}_{\mathbf{Gen}}(t) \\ \boldsymbol{\pi}_{\mathbf{Line}}(t) \\ \boldsymbol{\pi}_{\mathbf{Trafo}}(t) \end{pmatrix}. \quad (6)$$

We assume that generators, transmission lines, and transformers can fail and be repaired with the rates in Table 1 (Di Maio, Stincardini, and Zio 2022); therefore, the evolution of $\boldsymbol{\pi}_{\mathbf{Gen}}(t)$, $\boldsymbol{\pi}_{\mathbf{Line}}(t)$, and $\boldsymbol{\pi}_{\mathbf{Trafo}}(t)$ can be modelled by a binary Markov chain using the corresponding transition rates. At each time t, $\boldsymbol{u}(t)$ is passed to the OPF solver, which returns the optimal power generation setup and the voltage magnitudes and angles, defining the dynamical evolution of the variables considering the states of the components. If the OPF cannot be solved, we assume a full power outage, yielding zero active and reactive power generation.

The IP&TLC behavior is modelled and simulated in Python using the AC OPF solver of Pandapower (Thurner et al. 2018). We consider a time step of $\Delta t = 15$ minutes, which matches the TERNA sampling rate and a mission time of 100[h], allocating a fixed computational time of 6[h], which is enough to simulate at least one hundred scenarios, that will be used for benchmark. Simulations are performed on an Intel i7 9750H computer at 2.2 GHz.

Table 2 Threshold values considered for each IF

IF	Thresholds
ϕ_1	{0.00, 3.49, 11.83, 40.70, 140.00, 144.26, 158.23, 217.84, 472.40}
ϕ_2	{0, 1,2,3,4,5,6,7,8}
ϕ_3	{0.00, 3.49, 11.83, 40.70, 140.00, 144.26, 158.23, 217.84, 472.40}
ϕ_4	{0.00, 3.24, 3.50, 4.30, 5.62, 7.47, 9.85, 12.76, 16.20}

3.1. *Importance functions*

We list four IFs that will be used for comparison of the results. In all cases, we consider a fixed number of retrials $R_i = 4$, for any threshold level $i \in \{1,2, \dots\}$, whereas the number of main trials R_0 is not set since we let the scenarios generation continue until the computational time of 6 [h] is reached.

Power generation mismatch (ϕ_1)

Let $\mathbf{s}(t)$ and $\mathbf{s}^{\text{ref}}(t)$ be the actual and reference complex power generations vectors at time t, respectively. ϕ_1 is the module, at each time t, of the total differences between their apparent powers:

$$\phi_1(t) = \sum_{i \in \mathcal{G}} \left| |\mathbf{s}_i(t)| - \left|\mathbf{s}_i^{\text{ref}}(t)\right| \right|,$$

ϕ_1 is zero if the actual system condition is equal to the reference one (normal conditions); $\phi_1 > 0$, otherwise. The thresholds to be used in RESTART to spoon the retrials (see Table 2, 1st row) are set by sorting in ascending order the active maximum power ratings P_j^+ of each generator $j \in \mathcal{G}$, and then, calculating $T_{j+1} = P_{j+1}^+ + T_j$, with $T_0 = P_0^+$; in between T_j and T_{j+1}, $n_T > 0$ thresholds are added, that are quadratically distanced from the one previously added.

Down components (ϕ_2)

$\phi_2(t)$ counts, at each time t, the number of failed components along the scenario evolution:

$$\phi_2(t) = \#\text{ of failed components at time } t.$$

Since ϕ_2 can take values 0, 1, 2, …, we set the thresholds (see Table 2, 2nd row) to integer values, starting from zero.

Table 3 Computational effort for different scenario generation methods

	MC		RESTART		
	$n_{\text{sim}} = 40648$ (**)				
IF	$\xi(T_1)$	$\xi(T_2)$	$\xi(T_1)$	$\xi(T_2)$	n_{sim}
ϕ_1	0.0129	0.008	0.8327	0.8325	30280 (*)
ϕ_2	0.0653	0.0059	0.3254	0.0548	32287 (*)
ϕ_3	0.0	0.0	0.0	0.0	32193 (*)
ϕ_4	0.4667	0.1974	0.9683	0.8921	38218 (**)

(*), (**) Run in parallel.

Energy Not Supplied (ϕ_3)
$\phi_3(t)$ computes, at each time *t,* the cumulative sum of the differences between the actual active power $\mathbf{p}_j(t)$ delivered to the j-th customer and its demand $\bar{\mathbf{p}}_j(t)$, i.e., the lack of energy:

$$\phi_3(t) = \sum_{j \in \mathcal{C}} \left(\mathbf{p}_j(t) - \bar{\mathbf{p}}_j(t) \right) \quad \text{if } \mathbf{p}_j(t) < \bar{\mathbf{p}}_j(t),$$

Network vulnerability (ϕ_4)
$\phi_4(t)$ is that defined in Eq. (4) (see Section 2.2).

3.2. *Results*

Table 3 shows the different values of ξ when, without loss of generality, the two lowest thresholds $i = \{1, 2\}$ are considered: ξ is calculated with respect to the benchmark batch of simulations generated by MCS and by RESTART when driven by ϕ_1, ϕ_2, ϕ_3, and ϕ_4. In the Table, we also report the number of simulation points n_{sim} generated by the overall procedure.

For the case of MC, $\xi(T_1)$ is much larger than $\xi(T_2)$ for all the IFs, meaning that MCS allocates computational efforts in simulating lower importance zones (i.e., normal conditions that are not significant for the sake of training a BBM). This is evident in the case of ϕ_3 (ENS), which is equal to zero, meaning that the simulation never explores scenarios in which customers are not supplied with energy. In general, $\xi(T_1)$ and $\xi(T_2)$ for ϕ_4 are larger, suggesting that ϕ_4 seems to be more suitable for relevant scenario exploration.

For the case of RESTART, ξ is generally larger than for MCS. Thus, RESTART is effectively exploring more relevant regions. In particular, ϕ_4 is the IF with the highest $\xi(T_1)$, implying that most of the computational effort is allocated in relevant regions, i.e., above the first threshold. Besides, it explores the considered regions equally, i.e., the small reduction of $\xi(T_2)$ with respect to $\xi(T_1)$ suggests a good setting of the threshold values. On the other hand, ϕ_1, ϕ_2, and ϕ_3 are only positive when a disruption occurs. Indeed, the actual OPF solutions differ from those in normal conditions to account for the new topology of the power grid and provide a new optimal control input, yielding importance values different than zero only in those occasions. This is not ideal since when nothing happens, RESTART will act equivalent to MCS.

Another issue is related to the reference value used in the difference (that in normal conditions), since we must simulate this reference at least once, which can be time consuming. Besides, such reference corresponds to one realization of the external stimuli; therefore, we are forced to use this realization throughout the new retrials so that the comparison makes sense. These issues do not arise using ϕ_4. In fact, it is always greater than zero, increasing during those times of the day where the components are used more.

To conclude, ϕ_4 seems effective to drive RESTART for the generation of relevant scenarios of CPSs.

4. Conclusions

In this work, we tailor RESTART to the problem of generating relevant scenarios of CPSs behaviors. We do it so by introducing a novel dynamic IF that combines a centrality metric of the CPS components with their susceptibility to failure. A case study regarding an IP&TLC CPS confirms that i) the exploration of RESTART depends strongly on the selected IF, ii) typical vulnerability metrics are not suitable for guiding RESTART in the task of generating significant scenarios, and

iii) the novel IF here proposed is, instead, effective. Future work will consist in using the generated scenarios to train the BBM of the CPS GBM.

Acknowledgments

The project leading to this application has received funding from the European Union's Horizon 2020 research and innovation program under the Marie Skłodowska-Curie grant agreement No 955393.

References

Ansari, O A, C Y Chung, and E Zio. 2021. "A Novel Framework for the Operational Reliability Evaluation of Integrated Electric Power–Gas Networks." *IEEE Transactions on Smart Grid* 12 (5): 3901–13.

Cadini, F, D Avram, N Pedroni, and E Zio. 2012. "Subset Simulation of a Reliability Model for Radioactive Waste Repository Performance Assessment." *Reliability Engineering & System Safety* 100: 75–83.

Cassottana, Beatrice, Muhammad M Roomi, Daisuke Mashima, and Giovanni Sansavini. 2023. "Resilience Analysis of Cyber-physical Systems: A Review of Models and Methods." *Risk Analysis*.

Dang, Chao, Marcos A. Valdebenito, Matthias G.R. Faes, Jingwen Song, Pengfei Wei, and Michael Beer. 2023. "Structural Reliability Analysis by Line Sampling: A Bayesian Active Learning Treatment." *Structural Safety* 104 (September): 102351.

Devineni, P, B Kay, H Lu, A Tabassum, S Chintavali, and S M Lee. 2020. "Toward Quantifying Vulnerabilities in Critical Infrastructure Systems." In *2020 IEEE International Conference on Big Data (Big Data)*, 2884–90.

Di Maio, Francesco, Chiara Pettorossi, and Enrico Zio. 2023. "Entropy-Driven Monte Carlo Simulation Method for Approximating the Survival Signature of Complex Infrastructures." *Reliability Engineering & System Safety* 231: 108982.

Di Maio, Francesco, Alessandro Stincardini, and Enrico Zio. 2022. "Identification of Vulnerabilities in Integrated Power-Telecommunication Infrastructures: A Simulation-Based Approach." In *Proceedings of the 32nd ESREL Conference*.

Di Maio, Francesco, and Enrico Zio. 2017. "Dynamic Accident Scenario Generation, Modeling and Post-Processing for the Integrated Deterministic and Probabilistic Safety Analysis of Nuclear Power Plants." In *Advanced Concepts in Nuclear Energy Risk Assessment and Management*, World Scientific, Volume 1:477–504. Modern Nuclear Energy Analysis Methods.

Eusgeld, Irene, Wolfgang Kröger, Giovanni Sansavini, Markus Schläpfer, and Enrico Zio. 2009. "The Role of Network Theory and Object-Oriented Modeling within a Framework for the Vulnerability Analysis of Critical Infrastructures." *Reliability Engineering & System Safety* 94 (5): 954–63.

Futalef, Juan-Pablo, Francesco Di Maio, and Enrico Zio. 2022. "Grey-Box Models for Cyber-Physical Systems Reliability, Safety and Resilience Assessment." In *Proceedings of the 32nd ESREL Conference*.

Kroese, D.P., T. Taimre, and Z.I. Botev. 2011. "Variance Reduction." In *Handbook of Monte Carlo Methods*, 347–80. John Wiley & Sons, Ltd.

Newman, M E J. 2005. "A Measure of Betweenness Centrality Based on Random Walks." *Social Networks* 27 (1): 39–54.

Peherstorfer, B, K Willcox, and M Gunzburger. 2018. "Survey of Multifidelity Methods in Uncertainty Propagation, Inference, and Optimization." *SIAM Review* 60 (3): 550–91.

Piccinelli, R, G Sansavini, R Lucchetti, and E Zio. 2017. "A General Framework for the Assessment of Power System Vulnerability to Malicious Attacks." *Risk Analysis* 37 (11): 2182–90.

Terna. 2023. “Transparency Report: The Dashboard.” 2023.

Thurner, L, A Scheidler, F Schäfer, J -H. Menke, J Dollichon, F Meier, S Meinecke, and M Braun. 2018. “Pandapower—An Open-Source Python Tool for Convenient Modeling, Analysis, and Optimization of Electric Power Systems.” *IEEE Transactions on Power Systems* 33 (6): 6510–21.

Turati, Pietro, Nicola Pedroni, and Enrico Zio. 2016. “Advanced RESTART Method for the Estimation of the Probability of Failure of Highly Reliable Hybrid Dynamic Systems.” *Reliability Engineering & System Safety* 154: 117–26.

Villén-Altamirano, J. 2014. “Asymptotic Optimality of RESTART Estimators in Highly Dependable Systems.” *Reliability Engineering & System Safety* 130: 115–24.

Villén-Altamirano, Manuel, and José Villén-Altamirano. 2011. “The Rare Event Simulation Method RESTART: Efficiency Analysis and Guidelines for Its Application.” In *Network Performance Engineering: A Handbook on Convergent Multi-Service Networks and Next Generation Internet*, 509–47. Berlin, Heidelberg: Springer Berlin Heidelberg.

Zio, E. 2018. “The Future of Risk Assessment.” *Reliab. Eng. Syst. Saf.* 177: 176–90.

Zio, Enrico. 2013. *The Monte Carlo Simulation Method for System Reliability and Risk Analysis*. *Springer Series in Reliability Engineering*.