High-performance computing enabled contingency analysis for modern power networks

Alexandre Gràcia-Calvo, Francesca Rossi, Eduardo Iraola, Juan Carlos Olives-Camps, *Member, IEEE,* and Eduardo Prieto-Araujo, *Senior Member, IEEE*

***Abstract*—Modern power networks face increasing vulnerability to cascading failures due to high complexity and the growing penetration of intermittent resources, necessitating rigorous security assessment beyond the conventional $N-1$ criterion. Current approaches often struggle to achieve the computational tractability required for exhaustive $N-2$ contingency analysis integrated with complex stability evaluations like small-signal stability. Addressing this computational bottleneck and the limitations of deterministic screening, this paper presents a scalable methodology for the vulnerability assessment of modern power networks, integrating $N-2$ contingency analysis with small-signal stability evaluation. To prioritize critical components, we propose a probabilistic Risk Index (R_i) that weights the deterministic *severity* of a contingency (including optimal power flow divergence, islanding, and oscillatory instability) by the *failure frequency* of the involved elements based on reliability data. The proposed framework is implemented using High-Performance Computing (HPC) techniques through the PyCOMPSs parallel programming library, orchestrating optimal power flow simulations (VeraGrid) and small-signal analysis (STAMP) to enable the exhaustive exploration of massive contingency sets. The methodology is validated on the IEEE 118-bus test system, processing more than $57\,000$ scenarios to identify components prone to triggering cascading failures. Results demonstrate that the risk-based approach effectively isolates critical assets that deterministic $N-1$ criteria often overlook. This work establishes a replicable and efficient workflow for probabilistic security assessment, suitable for large-scale networks and capable of supporting operator decision-making in near real-time environments.**

***Index Terms*—Power System Reliability, Risk Assessment, N-2 Contingency, High Performance Computing, Risk index**

I. Introduction

Modern power networks are becoming increasingly complex, which heightens their vulnerability and necessitates rigorous assessment of their security posture [1] against cascading failures initiated by simultaneous outages ($N-2$ contingencies). Conventional security analyses typically focus on single-outage scenarios ($N-1$) and often overlook the combined effects of multiple concurrent outages, which may have been the root cause of large-scale historical blackouts, such as the one that occurred on 28 April 2025 in Spain and Portugal [2]. The increasing penetration of decentralized renewable energy sources and fast power electronics interfaced devices further complicates stability analysis [3], making system vulnerability assessment under severe multiple contingencies a critical task for grid operators.

The comprehensive assessment of $N-k$ contingencies has evolved primarily along three main axes: *security assessment methodologies*, *risk integration*, and *computational acceleration*. Traditional deterministic contingency screening, while foundational, is often insufficient for modern complexity, prompting a shift toward *probabilistic security assessment (PSA)* which integrates component reliability data [4]–[7]. Previous works have successfully deployed Monte Carlo and probabilistic methods to rank risks based on power flow violations or transient stability criteria [8]–[11]. However, these approaches often use simplified system models or fail to capture the full spectrum of post-contingency failure modes. A particularly persistent challenge is the integration of *small-signal stability (SSS) analysis*, which is essential for detecting growing oscillatory modes, into exhaustive probabilistic frameworks [12], [13]. While tools for automated SSS modeling exist [14], they are computationally intensive. Furthermore, the explicit modeling of structural failure modes, such as *system islanding*—a common precursor to cascading collapse—is frequently overlooked in large-scale screening methodologies. Addressing the computational load, High Performance Computing (HPC) has been successfully demonstrated to scale dynamic security assessments [15], though integrating this acceleration with open-source power flow platforms [16] and rigorous linearized EMT-based stability analyses for exhaustive $N-2$ evaluation remains a crucial implementation gap. Our work addresses these combined challenges:

1) We move beyond $N-1$ and partial screening to provide an *exhaustive $N-2$ analysis* of the test system.
2) We define a *multi-criteria risk index (R_i)* that uniquely combines optimal power flow divergence, islanding, and, critically, small-signal instability.
3) We demonstrate a replicable *HPC parallelization strategy* using PyCOMPSs to make this complex, multi-criteria, and exhaustive analysis computationally tractable.

This work presents a *systematic and scalable methodology* for performing exhaustive $N-2$ contingency analysis, with the capacity to assess the impact on operational security through *optimal power flow*, *small-signal stability*, and *islanding detection* (a multi-criteria scoring). The methodology is evaluated and validated on the IEEE 118-bus test system [17], where results demonstrate the efficacy of the new probabilistic risk index compared to classic deterministic security criteria. Specifically, we assess *both single ($N-1$) and simultaneous double ($N-2$) outages* in AC lines, transformers and generators by *modeling the post-contingency optimal power flow*

The authors are with CITCEA-UPC and BSC, Barcelona, Spain. E-mail: alexandre.gracia@upc.edu, francesca.rossi@upc.edu, eduardo.iraola@bsc.edu, juan.carlos.olives@upc.edu, eduardo.prieto-araujo@upc.edu

Manuscript received November X, 2025; revised December X, 2025.

and subsequently analyzing the eigenvalues of the linearized system state model to determine its stability. The ultimate goal is to define a robust and *probabilistic ranking of the network's critical components*.

The contributions of this paper are:

- The definition and validation of a probabilistic *multi-criteria Risk Index (R_i)*, which systematically combines AC optimal power flow feasibility, small-signal stability, and islanding criteria into a single risk metric weighted by component failure frequency.
- Exhaustive processing of 57 122 scenarios (encompassing single $N-1$ and ordered double $N-2$ outages), which serves as the foundational data set for the development and validation of the proposed probabilistic *Risk Index* (R_i).
- Implementation of a replicable *HPC parallelization strategy* using the PyCOMPSs framework, ensuring that this complex, multi-criteria, and exhaustive analysis achieves scalability for potential execution within operational time-frames (below 15 minutes).

The proposed methodology is tested and validated using the *IEEE 118-bus test system*, a medium-sized yet highly interconnected benchmark network. This validation involves the exhaustive processing of 57 122 *contingency scenarios* (covering all $N-1$ and ordered $N-2$ outages), which represents a significant computational challenge. By successfully managing this massive scope, the framework demonstrates its effectiveness and scalability in identifying critical assets and providing a realistic risk ranking for modern power networks.

The paper is organized as follows. Section II provides a detailed description of the proposed *Methodology*, including the exhaustive contingency analysis, the multi-criteria severity assessment (power flow, small-signal stability, and islanding), and the probabilistic Risk Index formulation. Section III details the *HPC-Enabled Parallel Implementation* using PyCOMPSs. Section IV introduces the *Case Study and Simulation Tools* (the IEEE 118-bus test system and specific reliability data). Section V presents the *Results and Discussion*, including the contingency coverage, stability analysis, and the computed critical component ranking based on R_i, along with operational implications and future proposals. Finally, Section VI provides the *Conclusion and Future Work*.

II. Methodology

A. Exhaustive Contingency Analysis

The first step is to identify all the elements in the network that could fail, as well as all the possible combinations of two elements that could fail simultaneously. In particular, we consider contingencies involving transmission lines, power transformers and generators. The following procedure is implemented to determine under what contingencies the system cannot be operated:

1) Start from the base state of the system, compute the pre-contingency optimal power flow, and verify that the system is initially stable to establish a reference.
2) For each element i (line, transformer or generator) in the network:
    a) $N-1$ **contingency (first outage):** Simulate the outage of element i, compute the optimal power flow, perform small-signal stability analysis, check for island formation, and store the results.
    b) For each remaining element j such that $j \neq i$:
        i) $N-2$ **contingency (second outage):** With i already out, simulate the outage of j. Compute optimal power flow, assess small-signal stability, check for islands and store results.
        ii) Restore element j to service.
    c) Restore element i to service.
3) Analyze the complete set of results to identify the most critical elements.

As indicated in the algorithm, during each contingency simulation we check for possible separation into electrical islands. In general, a division of the system into multiple areas can affect the analysis: often, only the main island interconnected to the largest generation should be taken as reference. In this initial stage, any scenario that results in islanding is marked as critical and kept in the study for specific revision afterwards.

B. Multi-Criteria Severity Assessment

The severity, $S_c \in \{0,1\}$, of a post-contingency state c is determined by the consideration of distinct criteria. For the contingency to be classified as severe ($S_c = 1$), at least one of the following conditions must be fulfilled:

1) Optimal Power Flow Feasibility and Operational Limits: A contingency c is considered severe if the AC optimal power flow solution does not converge, suggesting a structurally non-feasible operating point, or if the converged solution violates pre-defined operational limits (e.g., thermal limits, voltage bounds).

2) Small-Signal Stability Evaluation: To perform the small-signal analysis, we construct and linearize the complete system model at the operating point obtained from the optimal power flow solution. The general state-space formulation for small perturbations is applied, following established control theory principles for power systems [18].

Small-signal stability is assessed from the eigenvalues of the state matrix, and any contingency leading to at least one eigenvalue with non-negative real part ($Ri(\lambda_i) \geq 0$) is classified as unstable.

3) System Integrity: Islanding Detection: A key component in determining the severity of a contingency (S_c) is the structural integrity of the network. Any contingency, whether $N-1$ or $N-2$, that causes the fragmentation of the system into multiple electrical islands is considered a severe failure event. These islands may suffer from fatal generation-load imbalances or the loss of the slack bus, potentially leading to cascading collapse.

To evaluate this phenomenon, our methodology incorporates a topological connectivity analysis after each contingency simulation, based on graph-theoretic principles, in line with graph-based frameworks for vulnerability assessment in power systems [16], [19].

The procedure is as follows:

1) After simulating the disconnection of one or two elements, the numerical model of the network in its post-contingency state is generated.
2) A graph-analysis algorithm (similar to a Depth-First Search) is applied to the resulting topology to identify all connected subgraphs.
3) The number of electrically isolated subnetworks (islands) is then counted.

If the number of resulting islands is greater than one, the scenario is automatically classified as a failure of maximum severity ($S_c = 1$), and its associated risk (R_i) is computed accordingly. This ensures that any loss of network integrity is appropriately penalised in the final risk index.

Note on the applicability to $N-1$ analysis: Although the primary focus of this work is the exhaustive $N-2$ analysis, the proposed multi-criteria severity assessment and probabilistic framework remain highly valuable for single-outage ($N-1$) scenarios. Traditional $N-1$ security analysis often relies solely on steady-state limit violations. By integrating Optimal Power Flow (OPF) feasibility, structural islanding detection, and, critically, *small-signal stability (SSS)* evaluation into the severity score (S_c), the methodology provides a far more rigorous safety assessment for $N-1$ events. Furthermore, by utilizing component failure frequencies (λ_i), the resulting R_i index elevates the $N-1$ evaluation from a purely deterministic screening (where all severe failures are equally prioritized) to a *probabilistic risk ranking*, allowing operators to focus on the single component failures that contribute the most to the expected annual system risk.

C. Probabilistic Risk Index Formulation

To move from a purely deterministic analysis (where all failures are considered equally likely) to a probabilistic perspective, we weigh the severity of each contingency by its frequency of occurrence. The key concept is that

$$\textbf{Risk} = \text{Frequency} \times \text{Severity}.$$

For each network component i (line, transformer, or generator), one essential reliability parameter is required: the *failure rate* (λ_i), defined as the expected frequency of failures of component i (in failures per year) and related to the mean time to failure (MTTF) by $\lambda_i = 1/\text{MTTF}_i$.

We define the expected annual frequency for each contingency scenario:

1) $N-1$ **frequency (failure of i):** the failure rate of the component,
$$F_i = \lambda_i. \tag{1}$$
2) $N-2$ **frequency (failure of i and j):** the average rate at which j fails while i is already out of service (assuming independence),
$$F_{i,j} = \lambda_i \lambda_j. \tag{2}$$

It is essential to note that the frequency of an $N-1$ failure (e.g., 10^{-1} events/year) is several orders of magnitude higher than that of an $N-2$ failure (e.g., 10^{-5} events/year). This natural difference in frequency replaces the need for artificial weighting to prioritize $N-1$ failures.

The other important term for characterizing risk is severity. In this work, we define the severity of the i-th element as a binary variable whose value is obtained in the deterministic analysis. Specifically, $S_i = 1$ if the contingency of element i leads to a failure (non-convergence of optimal power flow, small signal instability, or undesired island formation), and $S_i = 0$ otherwise. When analyzing the failure of a second element j, the severity is denoted as $S_{i,j}$, but the value is obtained in an analogous manner.

The Risk Index for a component i R_i is computed as the sum of all risk contributions (frequency × severity) from every contingency scenario in which i participates, as follows:

$$R_i = F_i S_i + \sum_{j \neq i} F_{i,j} S_{i,j}, \tag{3}$$

where:

- R_i is the risk index for component i (failure-events/year),
- F_i is the $N-1$ failure frequency of i (i.e., λ_i),
- S_i is the severity of the $N-1$ failure of i (1 if failure, 0 otherwise),
- j denotes another component in the network ($j \neq i$),
- $F_{i,j}$ is the $N-2$ failure frequency of the pair (i, j) (i.e., $\lambda_i \lambda_j$),
- $S_{i,j}$ is the severity of the $N-2$ failure of (i, j).

It is important to note that (3) uses a *sum* to aggregate risk. The index R_i does not represent the risk of a single scenario, but rather the *total risk contribution* of component i to the system. It is therefore computed as the sum of the risk of the $N-1$ scenario (failure of i alone) plus the sum of all individual risks of the $N-2$ scenarios in which i is involved (failure of i together with any other component j). The resulting R_i has units of failure-events/year, representing the expected frequency of systemic failures in which component i is one of the contributors.

This index R_i captures the expected contribution of each component to the total number of systemic failures per year. A component with a high R_i is therefore more critical for the secure operation of the grid, either because it fails frequently (high F_i) or because its failure (alone or in combination) is particularly destabilising (high $\sum S_{i,j}$).

III. HPC-Enabled Parallel Implementation

Due to the large number of cases that had to be performed in the $N-2$ contingency analysis, the entire process has been parallelized using the PyCOMPSs framework from BSC [20]. PyCOMPSs [21], [22] is a Python-based programming environment that facilitates the definition of parallel tasks and their execution on distributed environments (HPC clusters, cloud). In our case, each contingency analysis (optimal power flow + stability analysis + island detection) is encapsulated as an independent task (typically requiring around 30 seconds depending on hardware conditions). Execution was performed on the Nord4 cluster at the Barcelona Supercomputing Center, allowing each contingency to be assigned a dedicated subset of cores for a short period in a burst of computational power.

This approach drastically reduced the total computation time: as resources are increased, the process scales almost linearly, in contrast to the exponential growth in the number of contingencies as their order increases. In parallel, we maintained a JSON file to store the results of each simulation (stability outcome, power flow and optimal power flow convergence, type of contingency—single or double—elements involved and whether islands were formed, etc.) without introducing I/O bottlenecks.

The general procedure is as follows:

1) Python functions that compute optimal power flows, build the stability model for each contingency, and detect islanding are written sequentially and decorated as PyCOMPSs tasks.
2) The PyCOMPSs runtime builds a dependency graph and schedules tasks across the available CPU cores.
3) After computation is completed, the results are collected and aggregated (convergence, stability, island detection, etc.).

This approach enables horizontal scaling of the exhaustive analysis to networks of the medium size and, potentially, larger systems, and lays the foundations for integrating a real-time decision-support assistant into the system operation center.

IV. Case Study and Simulation Tools

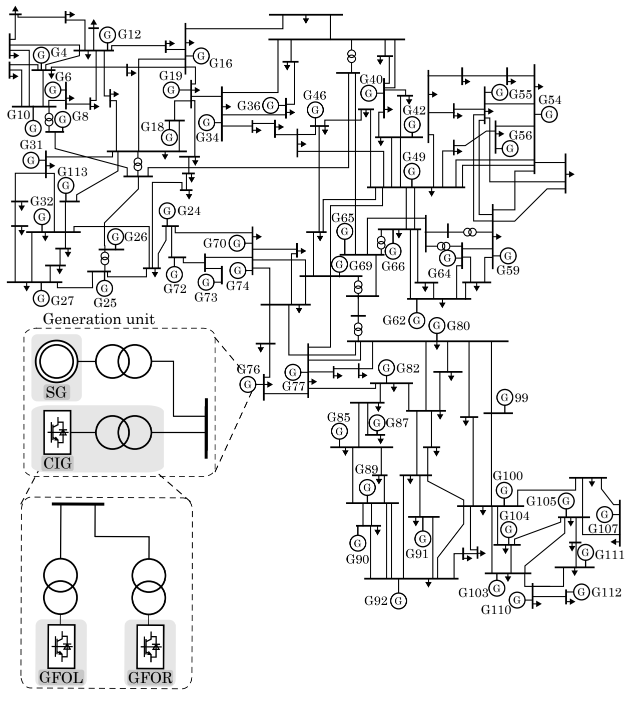

Fig. 1. Topological representation of the IEEE 118-bus test system.

This section presents the results of evaluating the proposed methodology on the IEEE 118-bus network [17], a classic benchmark system for power system stability and vulnerability assessment. The network consists of 118 high-voltage buses interconnected by 175 transmission lines and 53 generators or converters, and 11 transformers. Figure 1 presents a single-line diagram of the network. For optimal power flow simulation and contingency analysis we use VeraGrid [16], an open Python environment that includes tools for AC optimal power flow, OPF, and system dynamics. The base configuration is obtained through an AC optimal power flow, and island detection is performed using the VeraGrid framework. For small-signal stability analysis in EMT [14](STAMP Tool), we construct state-space linearized models of the entire system after each single and double contingency, incorporating generator dynamic equations and voltage regulation controls.

Since the IEEE 118-bus test case is a benchmark system lacking specific historical outage data, representative reliability parameters have been adopted based on standard values found in the literature [4], with generator failure rates specifically aligned with the IEEE Reliability Test System (RTS-96) [5]. These default values, summarized in Table I, are used to demonstrate the proposed methodology assuming typical failure characteristics for high-voltage components. It should be noted that, while uniform rates are applied here for this benchmark study, the proposed framework fully supports component-specific failure rates enabling the integration of real operational data.

TABLE I
Assigned Reliability Parameters

Component	**Failure rate (λ_i)**	**MTTF**
Lines	0.05 yr^{-1}	20 years
Transformers	0.02 yr^{-1}	50 years
Generators	0.10 yr^{-1}	10 years

V. Results and Discussion

A total of 57 122 contingency scenarios were evaluated, covering all $N-1$ and $N-2$ combinations considered in the study. Of these, 51 493 cases were classified as stable (or secure) according to the adopted criteria (optimal power flow convergence, absence of island formation and all eigenvalues with negative real part), which represents approximately 90.15 % of all analyzed scenarios. The remaining 5629 cases were identified as unstable (around 9.85 %), either due to divergence in the optimal power flow, the formation of electrical islands or small-signal instability detected through eigenvalue analysis.

These unstable situations correspond to contingency conditions in which the system loses operational security. The following subsections examine the distribution of these failures, the most relevant patterns observed and their implications for the computation of the risk index.

All 57 122 contingency cases were processed on the Nord4 HPC cluster [20]. We used 8 compute nodes, each with 48 CPU cores and 96 GB of main memory. Because the workflow consists of independent contingency evaluations, it parallelised efficiently across the cluster. The full analysis finished in about five hours of wall-clock time, indicating that the proposed method is computationally tractable at large scale.

It is worth noting that the method is *embarrassingly parallel*, and therefore its execution time can be reduced almost linearly by allocating additional computational resources. This aligns with the operator-support use cases discussed in the conclusions, where time budgets on the order of 15 minutes may be required.

A. Contingency Coverage and Stability

A total of 57 122 $N-1$ and $N-2$ contingency scenarios were analysed, including symmetric inverted combinations to ensure full coverage. The vast majority of these scenarios remain stable, except for approximately 1390 cases that resulted in numerical errors or non-convergent solutions. Most of these problematic cases appear to be associated with situations where the slack bus becomes isolated or located inside an island, which suggests that an alternative slack assignment could improve convergence reliability.

Among all $N-2$ simulations, a large proportion (90.15 %) converge successfully and show all eigenvalues with negative real parts, indicating small-signal stable post-contingency operation. By contrast, 9.85 % of scenarios exhibit at least one eigenvalue with positive real part, revealing small-signal instability or lead to the formation of one or more electrical islands, which we classify as severe events since they can lead to loss of reference, imbalance between load and generation, or cascading collapse.

These critical cases represent the most relevant patterns from the operational perspective, and they often correspond to specific structural weaknesses in the network topology.

The computation of the risk index R_i allows us to quantify how much each network component contributes to the overall likelihood of system failure. This provides a powerful tool for prioritizing maintenance, designing protection schemes, and preparing contingency strategies.

Overall, the IEEE 118 system shows a robustness level of approximately 90.15 % under $N-2$ analysis. However, the identified critical scenarios highlight that certain combinations of failures pose a significantly higher threat to operational security. These results offer a practical path for grid operators, who could focus their preventive actions on the small subset of components that dominate the system-level risk.

B. Interpretation of the Risk Index Values

The computed Risk Index (R_i) provides a quantitative measure of the expected contribution of each component to system-level failure events per year. Its interpretation is closely tied to both the reliability parameters (failure rates λ_i) and the observed severity of the simulated contingencies (S_c). Understanding the order of magnitude of R_i is essential for assessing the operational relevance of the results.

A value of R_i close to zero indicates that the component rarely participates in severe scenarios. This may occur for two distinct reasons: either the component has a low failure rate (large MTTF) or its individual outage and the combinations in which it participates do not lead to instability, island formation or loss of optimal power flow convergence. In practical terms, components with $R_i \approx 0$ have negligible impact on global security, even if they are part of the network topology.

On the other hand, values of the order of $R_i \approx 1.4$ represent a dramatically different situation. For example, a line with $R_i = 1.472$ contributes on average to almost one and a half severe system failures per year when accounting for both its $N-1$ and $N-2$ interactions. Since the failure rate of transmission lines is relatively low ($\lambda_i = 0.05$ year^{-1}), such a high value of R_i can only emerge when the component is involved in a very large number of $N-2$ contingencies with $S_{i,j} = 1$. This means that its structural position in the network makes it systematically part of combinations that reduce damping, induce instability or generate islands.

In this study, the resulting distribution of R_i spans approximately two orders of magnitude. The smallest values are below 10^{-3} failure events per year, typical of components that neither fail often nor lead to severe outcomes when they do. Intermediate values, in the range 10^{-2} to 10^{-1}, correspond mostly to generators and a subset of transformers with moderate participation in unstable combinations. Finally, the highest values, between 0.5 and almost 1.5 failure events per year, are dominated by transmission lines that appear repeatedly in severe $N-2$ combinations and whose reliability parameters amplify the accumulated risk.

These ranges illustrate that system-level vulnerability is not evenly distributed across the network. Instead, a small set of components produces most of the expected annual risk, while the majority contribute negligibly. This asymmetry is critical for prioritising maintenance, targeted monitoring and protection strategies.

C. Critical Components According to the Risk Index

Figures 2, 3, and 4 show the risk index R_i for lines, generators and transformers respectively. The combined ranking across all elements is presented in Fig. 5, which consolidates the global top 20 most critical components.

A clear pattern emerges in the combined ranking. The first seven positions correspond to transmission lines (IDs 113, 17, 12, 134, 137, 173 and 172), all with nearly identical values around $R_i \approx 1.47$ failure events per year, followed closely by Line 88 ($R_i \approx 1.45$). This similarity is not coincidental. It results directly from the uniform MTTF assigned to all transmission lines (20 years, corresponding to a failure rate $\lambda_i = 0.05$ year^{-1}). Since these lines also participate very frequently in severe $N-2$ combinations, the resulting products $\lambda_i \lambda_j$ accumulate to extremely similar R_i values. In these cases, the blue bars dominate, showing that the overwhelming majority of their risk contribution comes from $N-2$ interactions rather than from their individual $N-1$ outage.

Below this top cluster, a second tier appears. Line 39 has $R_i \approx 0.75$, followed by a group of three transformers (IDs 10, 9 and 0) with values between 0.56 and 0.59. Again, this pattern strongly reflects the reliability assumptions. Transformers were assigned an MTTF of 50 years ($\lambda_i = 0.02$ year^{-1}), which yields lower $N-1$ risk and reduced $N-2$ frequency. The resulting sharp drop between transmission lines and transformers illustrates how reliability parameters directly influence the probabilistic ranking.

Generators appear mostly in the lower half of the distribution. Generator 37 exhibits the highest generator risk ($R_i \approx 0.41$), almost entirely due to $N-2$ contributions. Generator 41 ($R_i \approx 0.30$) displays a significant red bar, showing that even its individual $N-1$ failure is classified as severe. The remaining generators (IDs 3, 13, 24, 26, 19 and 48) show much smaller R_i values, reflecting both their lower frequency

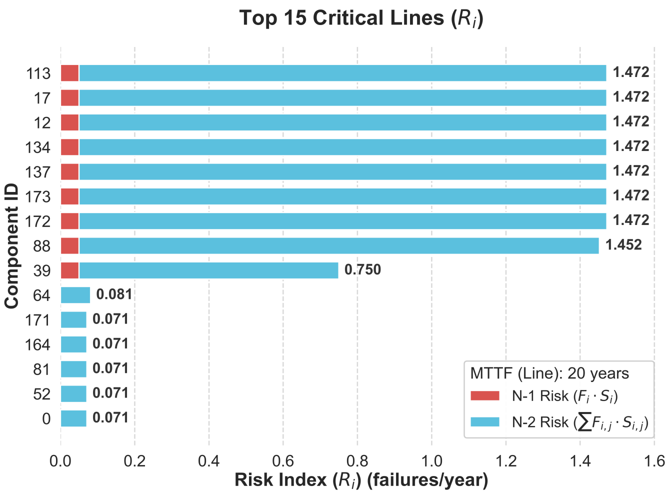

Fig. 2. Risk Index (R_i) for transmission lines.

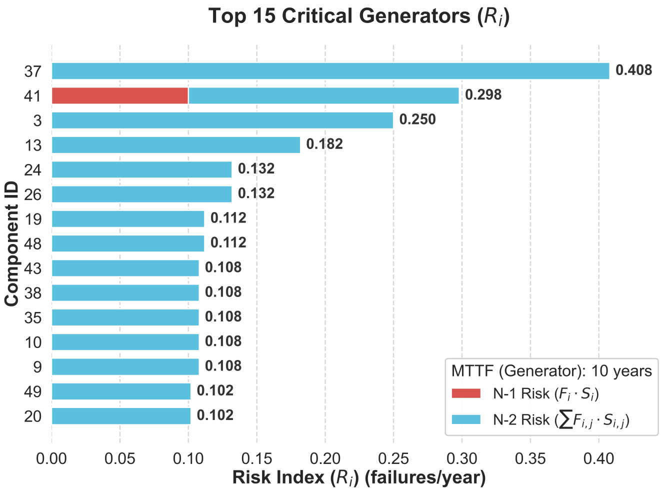

Fig. 3. Risk Index (R_i) for generators.

of participation in unstable $N-2$ scenarios and their higher assigned failure rate ($\lambda_i = 0.10$ year^{-1}, MTTF 10 years). This last point demonstrates an interesting phenomenon: despite generators having a higher intrinsic failure rate, they contribute far less to systemic instability than transmission lines. This means that, in this particular system, structural vulnerability is concentrated in the transmission network rather than in generation assets.

It is important to note that although we use category-wide default MTTF values for lines, transformers and generators, the implementation allows assigning individual MTTFs to specific components. This flexibility in the proposed methodology makes the risk index directly applicable to real systems in which reliability is heterogeneous and asset specific. By modifying element-level MTTF values, operators can immediately observe how the risk profile shifts as a result of ageing infrastructure, maintenance strategy or external environmental stressors.

The results demonstrate that system-level risk is highly concentrated in a small subset of components. Most of the expected annual failure events originate from combinations involving transmission lines, while transformers and generators play a secondary role. This highlights the importance of double-outage analysis. Many of the dominant contributions arise from $N-2$ severity rather than $N-1$ failures, which reinforces the need to evaluate interactions that are entirely invisible under a classical $N-1$ operational criterion.

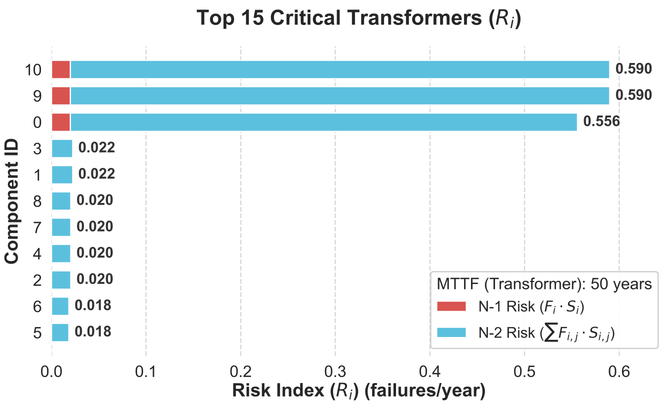

Fig. 4. Risk Index (R_i) for transformers.

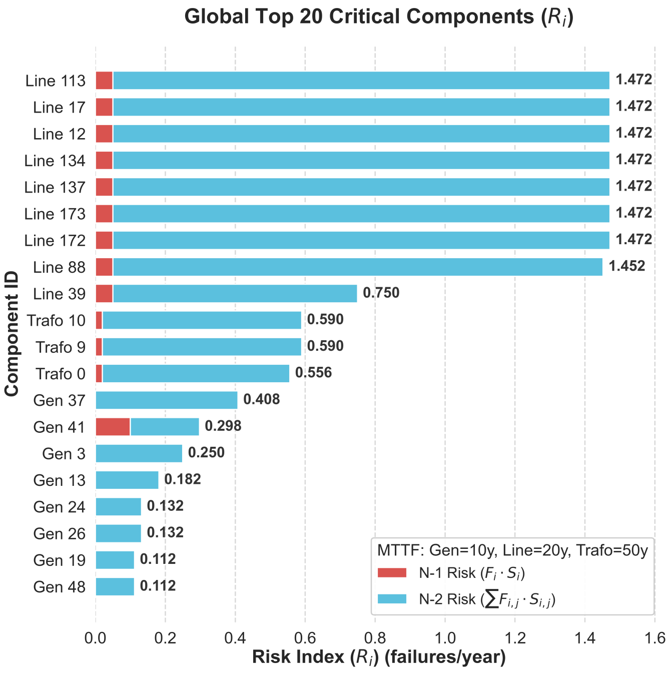

Fig. 5. Combined Risk Index (R_i) for all elements.

In practical terms, the risk index R_i helps operators distinguish between components that are statistically more likely to fail and those whose failures, even if rare, have disproportionate consequences. It provides a unified and quantitative framework to support asset prioritisation, maintenance planning and real-time contingency assessment.

Although this study focuses on $N-1$ and $N-2$ contingencies, real systems may experience more complex outage patterns. Nonetheless, $N-2$ contingency analysis combined with small-signal stability assessment offers a solid foundation for understanding real-world vulnerabilities. The structured methodology allows scalable analysis and future integration into operational practice, which is particularly valuable in contingency management.

This study demonstrates the feasibility of systematic $N-2$ analysis with small-signal stability evaluation on a medium-sized system. However, in larger networks the computational workload increases substantially and additional phenomena may arise.

A first-order probabilistic model has already been incorporated, using failure rates (λ_i) to weight contingency severity and compute the Risk Index (R_i). This risk-based (frequency × severity) perspective is more realistic than a purely deterministic ranking.

Several improvements could be explored:

- **Common-Cause Failures:** The current model assumes $N-2$ events are independent. In reality, storms or human errors may cause simultaneous failures (e.g., two lines on the same tower). Incorporating such probabilities would yield a more accurate $N-2$ risk estimate.
- **Non-binary Severity:** Severity is currently binary ($S_c \in \{0, 1\}$). A more refined model could treat severity as continuous, e.g., load shed in MW, voltage depression indices, or damping ratios, allowing differentiation between mild and catastrophic failures.
- **Uncertainty Analysis:** Failure rates λ_i are uncertain. A Monte-Carlo analysis on λ would enable confidence intervals for the risk ranking instead of a single point estimate.
- **Component-Specific Reliability:** The developed framework supports the assignment of specific MTTF values to each individual network element. Although this study applied uniform failure rates per asset class (lines, transformers, generators) for standardization purposes within the benchmark, the methodology is fully capable of processing heterogeneous reliability data. This allows for a more precise assessment in real-world scenarios where components exhibit varying failure probabilities based on their specific age, condition, or maintenance history.

In parallel, computational efficiency could be improved using machine-learning methods or heuristics to reduce the search space for preliminary screening of weak areas to filter out minor contingencies before running a full powerflow AC simulation. Further automation of islanding analysis (e.g., via reconnection heuristics or graph-theoretic tools such as improved Dijkstra variants) would also be beneficial.

D. Operational Implications of N-1 and N-2 Failures

From an operational perspective, the distinction between $N-1$ and $N-2$ contingencies is essential for understanding how the system should react to unexpected outages and how operators can anticipate cascading failures.

An $N-1$ failure corresponds to the outage of a single element, such as a transmission line, a transformer or a generator. Modern transmission systems are typically designed to withstand any $N-1$ event without losing operational security, meaning that voltage limits must remain acceptable, flows must continue to satisfy thermal limits and the system must preserve small-signal stability. When an $N-1$ contingency occurs, operators rely on predefined corrective actions that are well established in operational procedures. These actions may include generation rescheduling, activation of reserves, topology reconfiguration, re-dispatch of power flows through alternative paths or adjustments in voltage and reactive support devices. In most systems, these actions can be performed within a few minutes and do not require emergency procedures. Therefore, an $N-1$ failure is expected to be a manageable event that does not compromise overall system integrity.

In contrast, an $N-2$ contingency represents the simultaneous outage of two components. This type of event is much more challenging to handle because the consequences are harder to predict and the system may not be designed to tolerate such conditions under all operating states. An $N-2$ failure may lead to severe overloads on neighbouring elements, rapid voltage deterioration, loss of synchronism or the creation of electrically isolated islands. In such cases, corrective actions available to the operator become more restrictive. Actions that are feasible after an $N-1$ failure, such as rerouting flows or re-dispatching generation, may no longer be sufficient, especially if both outages affect major corridors or essential components. Emergency measures, such as controlled load shedding, temporary isolation of vulnerable areas or rapid reserve activation, may be necessary to stabilise the system.

The key difficulty is that $N-2$ failures often occur before operators have enough time to react to the initial $N-1$ event. If the system is already weakened by the first outage, the second outage can push it beyond its stability margin, leaving little time for corrective action. This highlights the importance of identifying the specific $N-2$ combinations that lead to instability or island formation, as these combinations reveal structural weaknesses that are hidden under classical $N-1$ analysis.

In summary, $N-1$ failures represent expected and generally manageable operational disturbances, while $N-2$ failures expose the system to high-impact situations that may require emergency actions and can escalate into cascading events. Understanding how each component contributes to these two classes of failures enables operators to prioritize preventive strategies, reinforce vulnerable areas and prepare focused response plans for the most critical multi-outage scenarios.

E. Real-Time Operator Support Tool

To bring the results of this analysis into operational practice, we propose an interactive operator support tool. Its goal is to integrate automated contingency calculations and risk indices (R_i) into a practical decision-support environment. In near real-time, the tool would highlight the most vulnerable components and suggest preventive or corrective actions. A simple graphical interface could include a network topology visualization, color-coded by element criticality (lines, transformers, generators), along with alarms or notifications when high-risk situations arise. This would facilitate rapid situational awareness and informed decision-making.

The tool should be structured into several modules:

- **Real-time data management:** Interfaces with operational data sources (SCADA) to obtain the current grid state (flows, generation, voltages, topology). It continuously updates internal models without interfering with ongoing operation.

- **Contingency simulation engine:** Integrates VeraGrid and HPC infrastructure to execute power-flow and small-signal stability calculations quickly. It could run in the background or on demand, automatically simulating the most relevant $N-2$ scenarios or enabling operator-driven what-if analysis.
- **Risk index computation and visualization:** Processes simulation outputs to compute the criticality index R_i for each element in near real-time. It highlights recurring unstable components and their associated severity, marking them as "hot spots". This information can guide operational actions (e.g., protective relays adjustment, control tuning, load reallocation).
- **Recommendation and visualization panel:** Provides an intuitive interface displaying network maps or graphs with risk indicators, lists of critical contingencies and suggested actions. For example, the most critical line or generator could be highlighted, with messages such as "reduce output", "activate reserves" or "redirect flows" based on predefined rules or prior analysis. It may also show time-evolution trends of critical eigenvalues or global R_i values.

A modular architecture could integrate these components through APIs or Python libraries with VeraGrid, along with a database for simulation logs and configurations. The essential goal is collaborative operation: giving operators near real-time guidance on the most dangerous multi-failure scenarios and suggesting preventive measures.

This bridges the gap between offline analysis and operational tools, turning the methodology into actionable decision-support.

VI. Conclusion and Future Work

We have presented a structured methodology for identifying critical components in the IEEE-118 system through exhaustive $N-2$ contingency enumeration, small-signal stability analysis and islanding detection. Using VeraGrid and Python, we modelled the impact of simultaneous outages on AC optimal power flow and subsequently constructed linearized EMT-based state-space models to assess dynamic stability. The analysis reveals that a non-negligible fraction of the $57\,122$ $N-1$ and $N-2$ combinations leads to instability or island formation, exposing specific components as systematic drivers of worst-case scenarios.

The proposed Risk Index (R_i) integrates deterministic severity and probabilistic failure frequency into a unified metric, enabling a meaningful ranking of components according to their expected contribution to system-level risk. Results show that risk is highly concentrated: a small subset of transmission lines dominates the global risk due to both their structural position in the network and the assumed reliability parameters (MTTF), while only a few transformers and generators make significant contributions. This aligns with the flexibility of the method, which allows individual MTTF assignments and can therefore adapt to real asset conditions in operational networks.

This probabilistic-deterministic framework offers a more realistic perspective than traditional $N-1$ security analysis, highlighting the importance of $N-2$ interactions that are otherwise invisible to classical operational criteria. The approach demonstrates strong potential to evolve into a proactive grid-security tool, capable of anticipating vulnerabilities and guiding targeted interventions. Future improvements include integrating real-world reliability data, exploring higher-order contingencies ($N-k$ with $k>2$), incorporating non-binary severity metrics and extending the methodology to larger or time-varying network conditions.

A particularly relevant direction is the development of a near real-time operator support system that embeds contingency simulation, risk index computation and graphical visualization. Thanks to HPC scalability and parallelisation, the full computational workflow could be executed within operational timeframes ($t < 15$ minutes), enabling informed decision-making and early warning mechanisms in control-room environments.

Overall, the proposed methodology not only deepens the theoretical understanding of multi-contingency security in networks such as IEEE-118 but also lays the foundation for practical tools with direct applicability in industrial and research settings. It creates a bridge between offline probabilistic risk assessment and actionable real-time operational support, while supporting a systematic, reproducible, quantitative way to identify vulnerabilities, prioritize mitigations, support operators, justify planning decisions, and explore the effects of failures.

Acknowledgment

The Project TED2021-130351B-C21 (HP2C-DT) is funded by MICIU/AEI/10.13039/501100011033 and by the European Union NextGenerationEU/PRTR.

References

[1] J. Breton, J. Jaskolka, and G. O. M. Yee, "An approach to determine a system's behavioral security posture" in *Foundations and Practice of Security*, K. Adi, S. Bourdeau, C. Durand, V. Viet Triem Tong, A. Dulipovici, Y. Kermarrec, and J. Garcia-Alfaro, Eds. Cham, Switzerland: Springer Nature Switzerland, 2025, pp. 94–110. doi: 10.1007/978-3-031-87499-4_7.

[2] European Network of Transmission System Operators for Electricity (ENTSO-E), "Grid Incident in Spain and Portugal on 28 April 2025," Public report, Oct. 2025. [Online]. Available: https://eepublicdownloads.blob.core.windows.net/public-cdn-container/clean-documents/Publications/2025/entso-e_incident_report_ES-PT_April_2025_06.pdf

[3] Y. Gu and T. C. Green, "Power System Stability With a High Penetration of Inverter-Based Resources," in *Proceedings of the IEEE*, vol. 111, no. 7, pp. 832-853, July 2023, doi: 10.1109/JPROC.2022.3179826.

[4] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*, New York: Springer, 1996, doi: 10.1007/978-1-4899-1860-4.

[5] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, "The IEEE Reliability Test System-1996," *IEEE Transactions on Power Systems*, vol. 14, no. 3, pp. 1010–1020, Aug. 1999, doi: 10.1109/59.780914.

[6] C. I. F. Agreira, S. M. F. de Jesus, S. L. de Figueiredo, C. M. Ferreira, J. A. D. Pinto i F. P. M. Barbosa, "Probabilistic Steady-State Security Assessment of an Electric Power System Using a Monte Carlo Approach," en *Proceedings of the 41st International Universities Power Engineering Conference*, 2006, vol. 2, pp. 408-411. doi: 10.1109/UPEC.2006.367509.

[7] S. Perkin, C. Hamon, R. Kristjansson, H. Stefansson and P. Jensson, "Framework for trajectory-based probabilistic security assessment of power systems," *IET Generation, Transmission & Distribution*, vol. 13, no. 7, pp. 1088–1094, Mar. 2019, doi: 10.1049/iet-gtd.2018.5396.

[8] E. J. da S. Pereira, J. T. Pinho, M. A. B. Galhardo, and W. N. Macêdo, "Methodology of risk analysis by Monte Carlo Method applied to power generation with renewable energy," *Renewable Energy*, vol. 69, pp. 347–355, Sep. 2014. doi: 10.1016/j.renene.2014.03.054.

[9] U. Shahzad and S. Asgarpoor, "Probabilistic risk assessment of an active distribution network using Monte Carlo simulation approach," in *Proc. North American Power Symposium (NAPS)*, 2019, pp. 1–6. doi: 10.1109/NAPS46351.2019.9000225.

[10] V. Donde, V. Lopez, B. C. Lesieutre, A. Pinar, C. Yang and J. Meza, "Severe multiple contingency screening in electric power systems," *IEEE Transactions on Power Systems*, vol. 23, no. 2, pp. 406–417, May 2008, doi: 10.1109/TPWRS.2008.919243.

[11] X. Zheng, S. Kotamarty, K. Thuerwaechter, A. Lee, S. H. Huang, and L. Xie, "A Generalized Approach to Contingency Screening with System Islanding," doi: 10.24251/HICSS.2023.342.

[12] S. Q. Bu, W. Du and H. F. Wang, "Probabilistic analysis of small-signal stability of power systems, a survey," in *Proc. Int. Conf. on Sustainable Power Generation and Supply (SUPERGEN 2012)*, Hangzhou, China, Jan. 2012, doi: 10.1049/cp.2012.1830.

[13] A. M. Tabrizchi and M. M. Rezaei, "Probabilistic small-signal stability analysis of power systems based on Hermite polynomial approximation," *SN Applied Sciences*, vol. 3, no. 9, art. 784, 2021, doi: 10.1007/s42452-021-04765-4.

[14] J. Arévalo-Soler, D. Moutevelis, E. Mateu-Barriendos, O. Alican, C. Collados-Rodríguez, M. Cheah-Mañe, E. Prieto-Araujo, and O. Gomis-Bellmunt, "A Matlab-based Toolbox for Automatic EMT Modeling and Small-Signal Stability Analysis of Modern Power Systems," arXiv:2506.22201, 2025. [Online]. Available: https://arxiv.org/abs/2506.22201

[15] I. Konstantelos, G. Jamgotchian, S. H. Tindemans, P. Duchesne, S. Cole, C. Merckx, G. Strbac, and P. Panciatici, "Implementation of a Massively Parallel Dynamic Security Assessment Platform for Large-Scale Grids," *IEEE Transactions on Smart Grid*, vol. 8, no. 3, pp. 1417–1426, May 2017. doi: 10.1109/TSG.2016.2606888.

[16] S. Peñate Vera, J. Fanals i Batllori, C. Alegre, benceszirbik, A. Blanco Castro, M. Lavoie, Q. Moya, L. Raiyan, B. Lüers, fernpos, M. Zsebeházi, J. Soler, ManuelNvro, ramferan, C. E. Fray, jag0nzalez, J. Gorcs, mmutto, peterkulik-navitasoft, R. Yu, "SanPen/VeraGrid: 5.4.0 VeraGrid first release (v5.4.0-veragrid)," Zenodo, 2025. DOI: 10.5281/zenodo.16971840. [Online]. Available: https://doi.org/10.5281/zenodo.16971840

[17] I. Pena, C. B. Martinez-Anido, and B.-M. Hodge, "An extended IEEE 118-bus test system with high renewable penetration," *IEEE Transactions on Power Systems*, vol. 33, no. 1, pp. 281–289, 2018 doi: 10.1109/TPWRS.2017.2695963.

[18] B. C. Pal and B. Chaudhuri, *Robust Control in Power Systems*, Springer, 2005. doi: 10.1007/b136490.

[19] I. B. Sperstad, E. H. Solvang and S. H. Jakobsen, "A graph-based modelling framework for vulnerability analysis of critical sequences of events in power systems," *International Journal of Electrical Power & Energy Systems*, vol. 124, art. 106408, Feb. 2021, doi: 10.1016/j.ijepes.2020.106408.

[20] Barcelona Supercomputing Center (BSC), "Nord4 overview," [Online]. Available: https://www.bsc.es/supportkc/docs/Nord4/overview/ [Accessed: Nov. 20, 2025].

[21] R. M. Badia, J. Conejero, C. Díaz, J. Ejarque, D. Lezzi, F. Lordan, C. Ramón-Cortés, and R. Sirvent, "COMP Superscalar, an interoperable programming framework," *SoftwareX*, vol. 3–4, pp. 32–36, Dec. 2015. doi: 10.1016/j.softx.2015.10.004.

[22] E. Tejedor, Y. Becerra, G. Alomar, A. Queralt, R. M. Badia, J. Torres, T. Cortes, and J. Labarta, "PyCOMPSs: Parallel Computational Workflows in Python," *The International Journal of High Performance Computing Applications*, vol. 31, no. 1, pp. 66–82, Jan. 2017, doi: 10.1177/1094342015594678.