Probabilistic Risk-Based Security Assessment of Power Systems Considering Incumbent Threats and Uncertainties

Emanuele Ciapessoni, Diego Cirio, *Senior Member, IEEE*, Gerd Kjølle, *Senior Member, IEEE*, Stefano Massucco, *Senior Member, IEEE*, Andrea Pitto, *Member, IEEE*, and Marino Sforna

***Abstract*—In-depth security analyses of power systems (PSs) require to consider the vulnerabilities to natural and human-related threats, which may cause multiple dependent contingencies. On the other hand, such events often lead to high impact on the system, so that decision-making aimed to enhance security may become difficult. Introducing the uncertainty, the risk associated to each contingency can be evaluated, thus allowing to perform effective contingency ranking. This paper describes an in-depth security assessment methodology, based on an "extended" definition of risk (including threats, vulnerability, contingency, and impact) aimed to perform the risk assessment of the integrated power and Information and Communication Technology (ICT) systems. The results of the application to test cases and realistic PSs show the added value of the proposed approach with respect to conventional security analyses in dealing with uncertainty of threats, vulnerabilities, and system response.**

***Index Terms*—Blackouts, contingency, extreme events, power systems, probability, risk, security, threats, vulnerability.**

I. Introduction

TRANSMISSION system Operators (TSOs) are more and more interested in pursuing the objective of a "resilient" power system: resilience has been defined in different contexts [1]–[3], but a quite agreed definition indicates resilience as "the ability of a power system to anticipate, absorb, adapt to and/or rapidly recover from a disruptive event" [3]. A major pillar to evaluate the resilience of a power system is the assessment of its security with respect to human-related and natural hazards, starting from the quantification of the likelihood and the impact of the threats, as well as the vulnerability of system components. To do this, TSOs need to adopt jointly-agreed security assessment methodologies [4], based on an "extended" risk concept to account for the threats, the vulnerabilities, the uncertainty of initiating events and of the power system response to disturbances (e.g., including protections and operators' behaviour).

Probabilistic risk based approaches have been adopted for many decades in power system planning [5], but are relatively new in security assessment, where N-1 criterion is still deemed as a good tradeoff between completeness and computational time. Though different risk based approaches to security assessment have been proposed by researchers in the last few years [6]–[10], the risk concept has been introduced only very recently by few operational standards to deal with extreme events. NERC Std. TPL-001-4 [11] suggests a list of single as well as multiple extreme events (e.g., loss of a substation or power plant) to measure power system performance in operational planning. NERC Std. CIP-014-1 [12] is being introduced to identify and protect transmission stations and substations and relevant control centers that –if affected by a physical attack– may lead to widespread disruptions and cascading outages.

In Europe, ENTSO-E [13] confirms the need to satisfy the N-1 criterion, but suggests a risk-based approach to quantify the opportunity to make the system secure against specific N-k, k>1 disturbances. Reference [14], which reports the state-of-art in cascading risk assessment, highlights the importance to deal with multiple contingencies –i.e., the main cause of cascading outages- and states that the identification of the most important cascades can benefit from the modeling of triggering causes (threats), from storms to sabotage: thus, the assessment of power system vulnerability to weather/environmental threats can help build a risk based approach to security. Some studies attempt to link current weather/environment conditions to power system reliability. In [15], a three-state weather model is presented to incorporate failures occurring in major adverse weather conditions. In [16], line failure rates are updated to the current weather conditions, while in [17] short term reliability indexes are calculated under different weather conditions. Reference [18] proposes an algorithm to assess power system resilience to extreme weather events through standard long term indicators, like Loss Of Load Expectation (LOLE), using sequential Monte-Carlo sampling and fragility curves to get component failure probabilities.

Manuscript received September 1, 2015; revised December 23, 2015; accepted January 6, 2016. Date of publication March 11, 2016; date of current version October 19, 2016. Paper no. TSG-01066-2015.

E. Ciapessoni, D. Cirio, and A. Pitto are with Ricerca sul Sistema Energetico S.p.A., Milan 20134, Italy (e-mail: emanuele.ciapessoni@rse-web.it; diego.cirio@rse-web.it; andrea.pitto@rse-web.it).

G. Kjølle is with SINTEF Energy Research (a Norwegian Research Center) Trondheim 7465, Norway (e-mail: gerd.kjolle@sintef.no).

S. Massucco is with the University of Genoa, Genoa 16145, Italy (e-mail: stefano.massucco@unige.it).

M. Sforna is with TERNA (the Italian TSO) Milan 20016, Italy (e-mail: marino.sforna@terna.it).

Color versions of one or more of the figures in this paper are available online at http://ieeexplore.ieee.org.

Digital Object Identifier 10.1109/TSG.2016.2519239

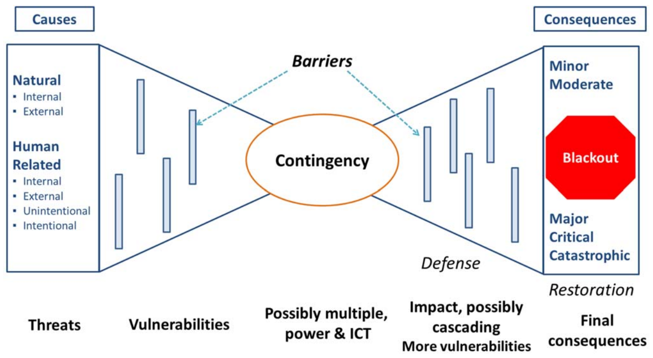


Fig. 1. Bow-tie diagram for AFTER methodology.

The present paper describes the novel in-depth security assessment methodology and tool, based on an extended risk approach, developed within the EU Project AFTER (*A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration*) [19]. The original aspects of the AFTER approach are: (1) the contingency selection based on current environmental/weather conditions; (2) the quantitative link between disturbance root causes and contingencies, by proposing an extension to classical definition of "risk". More in detail, the AFTER approach provides an algorithm to identify a subset of multiple, also dependent, "dangerous" contingencies which varies according to the current weather/environmental conditions: in this way, the N-1 criterion is complemented, avoiding combinatorial explosion in contingency analysis. The knowledge of the worst events which a power system is likely to face in the near future can be of paramount importance to improve the power system resilience, because it allows to improve the preparedness of operators and helps in elaborating suitable preventive actions. Secondly, the AFTER approach proposes a unified and general framework based on an extended definition of risk and aimed to quantitatively assess the link between the root causes of disturbances, i.e., threats (hazard, vulnerability assessment), and the initiating events themselves (contingency planning).

The paper is organized as follows: Section II presents the risk assessment methodology. Section III describes the threat/vulnerability modeling and contingency definition, tackling the important topic of the data needed to tune probabilistic models. Section IV illustrates the two-stage algorithm proposed to select the most risky single and multiple (also dependent) contingencies. Section V describes the assessment of the impact of contingencies on power system behavior, and provides the extended definition of risk. Section VI discusses the simulation results, and Section VII concludes.

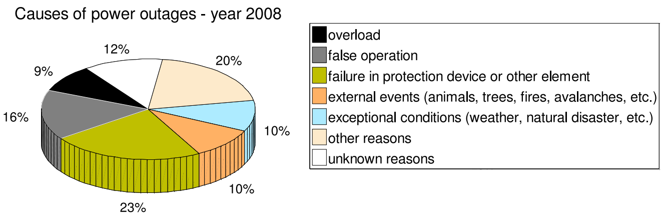


Fig. 2. Percentage contributions of main threats to the electric transmission faults in the UCTE Continental Europe (CE) area during 2008.

II. Probabilistic Risk Assessment: The "AFTER" Approach

The probabilistic risk assessment methodology developed within AFTER is based on the conceptual bow-tie model describing the relations between causes and consequences of unwanted events: Fig. 1 shows an example where the main unwanted events are contingencies potentially leading to cascading outages and blackouts, i.e., with severe (major, critical or catastrophic) consequences.

The left side shows the threat classification adopted in AFTER, which distinguishes natural threats from human-related threats, further classified into internal or external to the power system. The human-related ones are further classified into intentional (e.g. sabotage) or unintentional (human errors). This classification has been adopted after a preliminary investigation of statistical yearbooks available at [20] as well as of the final reports of recent blackouts aimed at identifying the main causes of service and infrastructure disruptions. As an example, Fig. 2 shows the contributions of the main threats, as percentages of the total number of events, to the disturbances in the UCTE (now ENTSO-E Continental Europe - CE) grid in 2008.

Threats may lead to a contingency through a set of causes exploiting vulnerabilities, while the contingency might lead to different consequences (impacts) through a set of circumstances. The initial impact may in turn affect other vulnerabilities, incepting a cascading process that finally results in a blackout. To catch this tight relationship between threats and contingencies, the classical concept of risk as a triple {contingency, probability, impact} is revisited and extended.

More specifically, in the modeling framework proposed by the AFTER approach [21] a threat can affect different vulnerabilities of ICT/power system components by activating stress variables[1] (e.g., a tornado induces additional mechanical forces to transmission line pylons). The stress in turn may cause the failure of a component. The generic 'contingency' at system level consists of the failure of one or more components. Vulnerability can be mathematically interpreted as the *conditional probability of failure of a component given the occurrence of a specific threat*. In turn, any *threat can also be described in probabilistic terms*; e.g., the probability of a natural threat, such as a lightning or a fire, depends on the weather or environmental conditions at the time of the event.

More details about the methodology and the prototype are provided in the next sections.

III. Threat and Vulnerability Modeling

This section describes in detail the probabilistic modeling of threats, of component vulnerabilities in the AFTER methodology, with a discussion on the availability of data sources for model tuning.

[1] Stress variables related to a threat indicate the physical quantities through which the threat affects the component vulnerabilities.

A. Modeling of Component Failures

The general formulation to evaluate the failure probability of one component due to a specific threat derives from probabilistic vulnerability and hazard assessment analyses [22]. The probability of failure P_F of a single component whose vulnerability is defined by a conditional probability function $P_V(t|\tau, s, x)$, between time instants t_0 and t, subjected to a single threat characterized by a {stress, time} multivariate probability density function (pdf) $p_{Thr}(\tau, s, x)$ can be expressed as:

$$P_F(x, t, t_0) = \int_{t_0}^{t} \int_S P_V(t|\tau, s, x) \cdot p_{Thr}(\tau, s, x) ds d\tau \qquad (1)$$

where:

- $P_F(x, t, t_0)$ is the probability that the component, located in x, fails *between* time instants t_0 and t;
- $P_V(t|\tau, s, x)$ is the conditional probability distribution that the component fails at time instant t due to value s of stress variable S (relevant to threat *Thr*) applied at time instant τ. Also component vulnerabilities are functions of time, due for instance to ageing or maintenance;
- $p_{Thr}(\tau, s, x)$ is the pdf of threat *Thr* applying value s of stress variable S in location x, at time τ. Term $p_{Thr}(\tau, s, x) ds\, d\tau$ is the probability to have stress s at time instant τ.

Upper-case letters are used for random variables (e.g., *S*) and lower-case letters for random variable realizations or non-random variables (e.g., *s*). Multivariate distributions in (1) should be properly characterized according to the component and the threat under study. The characterization process may present several problems due to the lack of sufficient statistical data available from the analyses of historical series or from real time monitoring systems. Assuming an “average model” of stress variable S applied to interval $\Delta t = t - t_0$ leads to (2):

$$P_F(x, \Delta t, t_0) = \int_S P_V^{(\Delta t)}(t_0, s, x) \cdot p_{Thr}^{(\Delta t)}(t_0, s, x) ds \qquad (2)$$

where apex $^{(\Delta t)}$ refers to the average (threat/vulnerability) model over time interval Δt. The interesting aspect of (2) is that it can be applied to different time frames, given that a suitable “average” model is available on a “Δt” basis. Next subsections will discuss the models adopted for $p_{Thr}^{(\Delta t)}$ and $P_V^{(\Delta t)}$ in the AFTER methodology.

Assuming constant failure rates within Δt relevant for operation (e.g., 15 minutes), a model of the probability of failure of multiple components, due to the same threat, is obtained by combining the “time to failure” exponential distributions of all the involved components according to probability laws. The more general case of multiple components subjected to multiple threats is also modeled, considering possible dependencies among threats.

This formulation provides a general framework for probabilistic modeling of power system contingencies. Special attention will be devoted to short term models, because the tool is mainly oriented to system operation; however, Section III.E also reports references which are especially useful for elaboration of long term threat models. In the following, only “single threat” scenarios are considered, without jeopardizing the generality of the approach.

TABLE I
STRESS VARIABLES FOR THE ANALYZED THREATS

Threat	**Stress variable [measurement unit]**	**Category**
Ice and snow	Wind+Ice load [N/mm^2] Conductivity on insulators [μS/cm^2]	Q2
Pollution	Pollution concentration on insulators [mg/cm^2]	Q1
Lightnings	Flash to ground density [# flashes/(km^2*h)]	Q1
Earthquake	Peak ground acceleration [m/s^2]	Q2
Physical malicious attacks	Attack scenario probability [# attacks/week]	Q2
Landslides	Newmark displacement [m]	Q2
Floods	Water level [m]	Q1
Fires	Insulation temperature [°C]	Q2
Vegetation	Tree height [m]	Q1
Thermal Ageing	Air temperature [°C]	Q1

B. Threat Classification and Modeling

The modelled threats may range from natural disasters (ice and snow storms, pollution, lightning, earthquakes, sabotage, earthquake-induced landslides, floods, fires, tree contact, component aging) to deliberate acts of sabotage.

Different sources of information can be used to refine the threat distributions in (2). The tool can exploit statistical analyses provided in literature for several natural threats. In addition, very short term models (15 minute ahead) of weather related threats should be tuned with data coming from real time monitoring systems. Due to their very low frequency, both intentional and unintentional human related threats can be characterized only via qualitative information from experts.

Poisson distributions for lightning-induced line outages [23], Bayes networks for animal-related (i.e., birds nesting on transmission lines, etc.) [24] or fires threats, and extreme value distributions for storm-induced ice and wind loads [25] and for floods [26] are some examples of long term probabilistic models.

C. Short Term Threat Models

The computation of the last term of (2) requires the knowledge of the dependence of the stress variable pdf on location x (*spatial dependence*). The AFTER methodology is general and can include an accurate representation of the stress variable if data from on-line monitoring systems are available. As for the spatial dependence issue, the investigation of the literature leads to identify two categories of threats:

- Q1: threats with “standard” probabilistic models
- Q2: threats with “customised” probabilistic models

TABLE I shows the correspondence between each threat and its major stress variable(s).

For Q1 category, the spatial distribution of the mean value of the stress is represented by means of a quite general expression, i.e., a Gaussian like function, given by (3) where s_1, s_2, are fixed parameters characterising the geographical extent of the stress; *AF* and *baseload* characterize the stress magnitude, while (x_c, y_c) is the "center of the stress".

$$f(x, y) = (AF - baseload) \times e^{-\left[\frac{(y-y_c)^2}{s_1}+\frac{(x-x_c)^2}{s_2}\right]} + baseload \quad (3)$$

The above parameters make the formula general enough to include both spatially spread phenomena (like pollution) and spatially limited phenomena (like a fire in a substation), and it can be further generalized by including the ellipsoidal distributions with their principal axes not parallel to *x*-*y* axes: current formulation in (3) -however- does not limit the generality of the proposed assessment framework. Without loss of generality, the standard deviation of a stress variable in a specific location is modelled as a percentage of the mean value of the stress itself and depends on the time horizon of analysis.

For Q2 category the spatial distribution of the mean and standard deviation of the stress variables is calculated as a function of scalar or vector fields of specific threat parameters considering different ad hoc "short term" models. For an ice and snow storm, stress variables (the mechanical loads and the ice-induced conductivity on insulators) are calculated by applying stochastic input parameters (wind speeds, precipitation rates, storm movement direction and speed) to the ice/snow storm model in [27]. The ground acceleration scalar field is estimated given the earthquake location and magnitude, using the attenuation law in [28]. The insulation temperatures for transformers are calculated using the hottest spot temperature method [29], while the Newmark displacements induced by earthquakes are usually distributed according to a uniform distribution between 0 and a maximum displacement, a function of the earthquake magnitude [30]. As for human related threats, human errors are probabilistically characterized using general methods, like the Performance Shaping Factors (PSF) [31]. Intentional attacks to ICT and power system, including acts ranging from physical attacks to power infrastructures to cyber-attacks to SCADA systems, may be modeled using semi-Markov chains, attack trees and Bayesian networks. The physical attack model in the AFTER methodology is based on Bayes networks, as in [32].

D. Vulnerability Modeling

In general, each component is characterized by a vulnerability function with respect to each threat. The vulnerability models used in (2) are obtained from: (a) ad hoc tests, like mechanical fragility curves, blast withstanding capacity curves, voltage withstanding capacity curves [33] for insulating materials; (b) mathematical models which link component properties to the exposure to specific threats, for examples rolling sphere method for exposure to lightning [34]; (c) qualitative information from experts or "ad hoc" drills, like vulnerability of a SCADA system, or of a substation to physical attacks. Vulnerability models may also include ageing processes, e.g., modeled via Arrhenius' law or combined electric-thermal stress models [35].

TABLE II
REFERENCES TO STATISTICAL ANALYSES FOR THREATS AND COMPONENT VULNERABILITIES

Component / Threats	OHL/ Cable	Transfos	Gens	Subs	Distribution networks
Ice & snow wind storm	[38][41] [25]	–	–	[49]	–
Lightnings	[38][40] [41][42]	[40][41]	[40] [41]	[40][41] [49][33]	[53]
Flood	–	–	–	–	[26]
Salt and pollution	[33][43]	[39][33] [43]	[33] [43]	[49][33] [43]	–
Fires / high temperatures	[44]	[39]	–	–	–
Animals	[24][51]	–	–	–	–
Vegetation	–	–	–	–	[45]
Earthquakes	[28]	[28]	[28]	[28]	–
Landslides	[30]	[30]	[30]	[30]	–
Ageing	–	[52][39]	–	[49]	[50][49]
Human errors	[31]	[39][31]	[31]	[31]	–
Malicious attacks	[46][47] [48]	[46][47]	[46] [47]	[46][47]	–

E. Data Issues for Model Tuning

The characterization of the probabilistic models is one of the main barriers for the application of probabilistic techniques in real world power system operation [36]. To this regard TABLE II collects interesting references which provide guidelines for statistical analyses of historical data and for the development of probabilistic models related to different threats and vulnerabilities of components/systems (from transmission equipment to distribution networks) with special focus on long/medium term horizons. It's worth noticing that the reliability data reported in the references of TABLE II are not used in the risk assessment analyses described in Section VI: short term threat models, as the ones used in Section VI, are tuned considering measurements of stress variables (e.g., wind speed, precipitation rate, etc.), available from technical disturbance reports concerning specific "real life" weather/environmental hazards.

Some interesting results have been derived from benchmarking the threat and vulnerability probabilistic models relevant to lightnings against real world data. As an example, from statistical analysis of real data [23], the yearly average failure rate $\lambda_{yearly\_average}$ of a 220 kV transmission line for the Italian system is $3.5{\cdot}10^{-10}$ failures/(km·s). Assuming 15 hours of severe storm in the region under study allows estimating the failure rate $\lambda_{BadWeather}$ over "bad weather" quarters of hour:

$$\begin{aligned}\lambda_{BadWeather} \cdot 15 \cdot 4\big[\text{quarters of hour}\big] &= \lambda_{yearly\_average} \cdot 365 \cdot 24 \cdot 3600 \\ &= 1.8 \cdot 10^{-4} \text{ nr flashes}/(\text{km} * \text{quarter of hour})\end{aligned}$$

This means $5.4{\cdot}10^{-5}$ failures/(quarter of hour) for any span of a line (assuming a 300 m long span for a 220 kV line).

The simulation of a severe lightning storm performed by the AFTER tool on a realistic 220 kV test grid, assuming a flash-to-ground density of 3.2 flashes/(h·km^2), realistic for severe storms as in [37], shows that the maximum 10-minute failure probability over the most exposed 300 m long span of a 220 kV line is $3.6{\cdot}10^{-5}$failures/(10 min), in good matching with the estimates from historical data.

IV. Contingency Selection: A Two-Stage Approach

The selection of the most "relevant" contingencies to be further analyzed includes two stages:

i. Selection of critical components via cumulative sum screening method [37]
ii. Screening of most "risky" contingencies using fast impact assessment techniques based on topological metrics

A. Selection of Critical Components (Stage I)

In the first stage all components are ranked based on their failure probability. The critical components (i.e., the ones "explaining" the largest fraction of total failure probability) are identified using a cumulative sum screening technique [37] which works as follows:

1. rank failure probability of all components into decreasing order, creating a map $M(l) = l'$ between l and l' (indexes of original and ordered components) s.t. $P_F^{(l')} > P_F^{(l'-1)}$
2. calculate the cumulative sum for each ordered component with index l' $F(l') = \sum_{h=1}^{l'} P_F^{(h)}$
3. Find line l^{TOT} whose F minimizes $|F(l^{TOT}) - \alpha \sum_{i=1}^{N} P_F^{(i)}|$ where α, the coefficient of the sum of failure probabilities of all N components, is called "fraction of explained total failure probability"
4. Get minimum failure probability threshold P_F^{TOT} as: $P_F^{TOT} = P_F^{M^{-1}(l^{TOT})}$
5. Select components with failure prob. higher than P_F^{TOT}.

B. Generation of Set of Single and Multiple Contingencies

After that, an enumeration technique is adopted to generate a set of single and multiple contingencies starting from critical components. Assuming constant failure rates within Δt, the "time to failure" probability distribution for each non-repairable component is given by an exponential Cumulative Distribution Function (CDF), as already mentioned in Section III.A: this is a valid assumption for short time intervals as the ones adopted in operation. The exponential distributions of the "time to failure" of all components involved in the contingency definition are combined by using probability theory laws and copula concept, to get the final distribution of the probability of occurrence of the contingency $P_{CTG}(t)$: the value of probability used in stage II of the screening process is the maximum value of $P_{CTG}(t)$ over the time interval Δt of interest, called $prob_{ctg}$ in the sequel of the paper. The calculation of the probability of occurrence for high order (N-k, k>1) contingencies, accounts for common mode and dependent events. Common mode events (like outage of k branches subject to the same storm) are analyzed thanks to the available geo-spatial model of the threat affecting the portion of the grid under study. Modelled dependent events consist in (a) busbar contingencies (also accounting for protection malfunction), (b) power plant contingencies and (c) double circuit line outages.

TABLE III
Dependent Branch and Busbar Contingencies With Probabilities of Occurrence

Contingency	**Probability $P_{CTG}(t)$**
Tripping of single line A of a double circuit i	$p_{i,A}(t) - C([p_{i,A}(t), p_{i,B}(t)], \rho_i)$
Tripping double circuit i	$C([p_{i,A}(t), p_{i,B}(t)], \rho_i)$
Only for separable bus bar in two half-busbar	
Tripping bays of half-busbar X (X = 1, 2) of busbar v	$1-\left[\begin{array}{l}(1-p_{HB_X}(t))\times \\ \times \prod_{i=\left\{\substack{\text{singlecircuit linesconnected} \\ \text{on thehalf-busbarX}}\right\}} (1-p_i(t)\cdot p_{CB_i,oc})\times \\ \times \prod_{k=\left\{\substack{\text{trippingsinglecircuit of} \\ \text{doublecircuit lines connected} \\ \text{on thehalf-busbarX}}\right\}} (1-(p_{k,A}(t)-C([p_{k,A}(t),\ p_{k,B}(t)], \rho_k))\cdot p_{CB_k,oc})\times \\ \times \prod_{j=\left\{\substack{\text{trasformers connected} \\ \text{on thehalf-busbarX}}\right\}} (1-p_{trafo_j}(t)\cdot p_{CB_j,oc})\end{array}\right]$
Tripping bays of the whole busbar	$p_{B_v}(t)\cdot(p_{BDP,oc}+p_{K,oc})$
Tripping double circuit i + bays of half-busbar of the faulted line i	$C([p_{i,A}(t), p_{i,B}(t)], \rho_i)\cdot p_{CB_i,oc}$

The rationale of the proposed contingency generation method is to link the failure probability of critical components to the probability of occurrence of contingencies. For example, a set of M critical branches is associated to:

- The multiple "common mode" (CM) branch contingencies: the probability of occurrence $P_{CTG}(t)$ of a specific configuration of m trippings and M-m non-trippings is given by (4)

$$P_{CTG}(t) = \prod_{l \in \Gamma^m} p_l(t) \times \prod_{l \in \bar{\Gamma}^m} [1 - p_l(t)] \tag{4}$$

  where $\bar{\Gamma}^m$ is the complementary set of Γ^m (subset of m tripped branches), and $p_l(t)$ is the probability distribution of the "time to failure" for branch/derived from the relevant failure probability $P_F^{(l)}$. The dependence on common cause is given by the single factors of the product (i.e., the branch failure probabilities) which all change accordingly to the extent and magnitude of the same threat, exploiting the available geo-spatial threat model.
- The multiple functional dependent contingencies which concern busbar systems of substations including the substations which interconnect power plants to the grid. In fact, the combination of a stuck breaker and a branch failure may lead to these contingencies. TABLE III reports the probability of the main dependent contingencies, focusing on double busbar systems.

The symbols adopted are listed below: $p_{Bv}(t)$ and $p_{HBx}(t)$ are respectively the failure probability of busbar v and half-busbar X, $p_{k,A}(t)$ the failure probability of circuit A of double-circuit line k, C and ρ_k are respectively the Gaussian copula and the relevant Pearson correlation coefficient for double circuit faults, $p_{trafo_j}(t)$ the failure probability of j-th transformer, $p_{CB_j,oc}$, $p_{BDP,oc}$ and $p_{K,oc}$ the "fail on command" probability respectively of j-th Circuit Breaker (CB), Bus Differential Protection (BDP) and bus coupler (K).

In particular, two failure modes of CBs are modeled:

- The "fail on command" probability $p_{CB_j,oc}$ defined in frequency terms, whose typical values can be found in literature surveys;

- The time varying "probability to fault" $p_{CB}(t)$ depending on environmental conditions and modeled through suitable vulnerability models in the methodology. Considering this failure mode, the quantity $p_{B_v}(t)$ for busbar v showing a failure probability of metallic bars equal to p_{MB_v}, and connecting $N_{CB,\,Bv}$ CB's and $N_{VT,\,Bv}$ Voltage Transformers (VT's) is given in (5). A similar equation holds valid for half-busbar failure probability.

$$p_{B_v}(t) = 1 - \left[\begin{array}{c} \left(1 - p_{MB_v}(t)\right) \times \prod\limits_{i=1\ldots N_{CB,\,Bv}} \left(1 - p_{CBi}(t)\right) \\ \times \prod\limits_{j=1\ldots N_{VT,\,Bv}} \left(1 - p_{VTj}(t)\right) \end{array} \right] \tag{5}$$

If a generator is found to be a "critical component", then the busbars of the relevant interconnecting substation are included in the set of critical components. In particular, the evaluation of the probability of occurrence of the relevant functional dependent contingencies accounts for the failure probability of generators themselves.

C. Contingency Screening (Stage II)

Contingencies are screened based on "ex-ante" risk indicators, which are defined by combining contingency probability with topological impact metrics, i.e., average inverse geodesic length [54] and net-ability [55], and their computation is very fast. The ex-ante metrics adopted are:

- *Average Inverse Geodesic Length* (AIGL) [54]:

$$AIGL = \frac{1}{N_B(N_B-1)} \sum_{i}^{N_B} \sum_{j \neq i}^{N_B} \frac{1}{d_{ij}}$$

  where d_{ij} is the electrical length of the shortest path between nodes i and j.
- *Net-Ability* (NETAB) indicator, exploiting the DC load flow and evaluating the level of congestion on the corridors between generators and loads [55]. In particular, the net-ability index is given by the following formula:

$$NETAB = \frac{1}{N_G N_D} \sum_{i \in \Theta} \sum_{j \in \Psi} C_{ij} \sum_{k \in H_{ij}} p_{ij}^{k} \frac{1}{d_{ij}^{k}}$$

  where Θ and Ψ are the sets of generator and load nodes respectively, while H_{ij} is the set of paths from generator i to load j; likewise N_G and N_D are the total numbers of generators and loads, respectively. Finally, p_{ij}^{k} is the power share of path k in transmitting power from i to j, and C_{ij} is the transfer capacity between generation node i and load node j.

The proposed screening algorithm provides several options to tune the selection of the contingency set, e.g., maximum "ex-ante" risk threshold and the fraction of "explained" total failure probability.

Each contingency is not only characterized by the set of components that are tripped to clear the fault, but also by the time sequence of the trippings themselves depending on the behaviour of primary and backup protections. Thus, when dynamic simulations are performed, the same "static" contingency defined in terms of tripped components may correspond to a set of different "dynamic" contingencies.

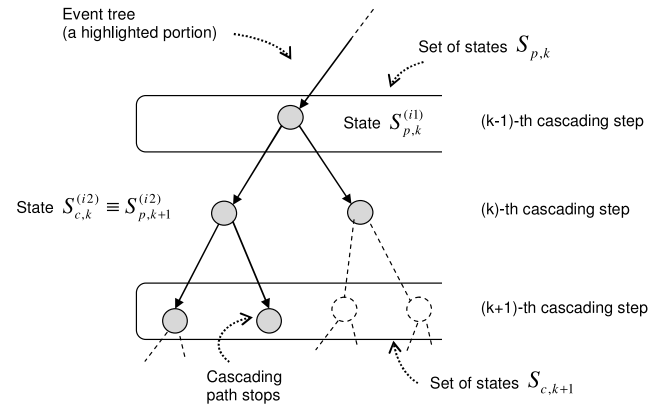


Fig. 3. Rationale of the algorithm to evaluate cascading path probability.

V. Modeling of ICT/Power System Response to Contingencies

After the contingency screening, the impact of each contingency is evaluated using a quasi-static cascading engine and/or a time domain simulator.

A. Impact Assessment

The cascading engine [56], [57], aimed to simulate at least the early stages of the cascade triggered by contingencies, uses probabilistic event trees to analyze a quite exhaustive set of cascading paths, accounting for hidden failures [58] and uncertain protection settings, and quantifying the impact (in terms of loss of load - LOL) and the probability of each path.

The evaluation of the probability of each cascading path over time t is based on the algorithm, illustrated in Fig. 3. Each "child" state at k-th cascading step belongs to set $S_{c,k}$ and it is generated by one of the states composing the set $S_{p,k}$ of "parent states" at (k-1)-th step. A transition from two subsequent cascading steps in the event-tree is characterized by a parent state (higher node of the event tree) and a child state (one of the lower nodes stemming from the "parent" node). The parent state at step 1 is the system state after the contingency application. The probability of having a certain child state $S_{c,k}^{(i2)}$ at latest at time t given a specific parent state $S_{p,k}^{(i1)}$ has occurred before time t is given by (6). The evaluation of the conditional probability of the whole cascading path is obtained by recursively applying (6), taking into account that the set of "parent states" for cascading step k+1 is a subset of the children states for step k.

$$P\left(t_{Sc,k^{(i2)}} \leq t,\, t_{Sp,k^{(i1)}} < t\right) = \int_{t_0}^{t} P_{Sc,k^{(i2)}}(t|\tau) \cdot p_{Sp,k^{(i1)}}(\tau) d\tau \tag{6}$$

where $p_{Sp,k^{(i1)}}(\tau)$ is the probability density function of the time instant of occurrence of parent state $S_{p,k}^{(i1)}$ while $P_{Sc,k^{(i2)}}(t|\tau)$ is the conditional probability that state $S_{c,k}^{(i2)}$ occurs at latest at time t.

The time domain simulator evaluates in detail the system dynamic response in the early seconds after each contingency, including primary and back up protection logics, i.e., the bus differential protection, distance relays (zones 1 and 2), overcurrent protection for transformers, breaker failure device.

B. Impact and Risk Indicators

Risk is classically defined as a triple {contingency, probability, impact} [6]. In the AFTER approach an extended concept of risk is introduced: risk is defined as a quadruple {threat, vulnerability, contingency, impact} where the "probability" term is replaced by the probability distributions associated to threats and vulnerabilities. The adopted definition allows to link PHA (Probabilistic Hazard Assessment) studies to SA (Security Assessment) analyses, moving the focus to the root causes of disruption events. This is a step forward with respect to classical PRA (Probabilistic Risk Assessment) approaches (like OL-RBSA [6]) where the probability of occurrence of the contingency is usually derived from historical data statistical analyses, and does not correspond to actual environmental conditions where power system operates. In particular, the adopted risk indicator is the expected value of the impact for the considered contingencies considering threats and component vulnerabilities [57]. The vulnerability of the components links the probabilistic model of generic threat Thr_p with the probability of occurrence of contingency *ctg*, while the vulnerability in the system response links contingency *ctg* with the final consequences (impact) on the power system itself. The action of threats on power system clearly depends also on the specific (current or forecast) power system operating conditions OC_j. In the present paper, the term "operating condition" includes both strictly operational conditions, i.e., load pattern, generation dispatch and network topology, and more general environmental conditions, like ambient temperature, wind speed. In any case, risk can be associated to:

1. a specific contingency (deemed as "dangerous" in the specific operating point subject to the given threat): *contingency risk* indicators help operators focus on events with highest risk (to plan suitable control actions)
2. the operating condition and the set of "dangerous" contingencies: *global* indicators assess how *system risk* changes under varying threats.

In the following, some examples are reported to demonstrate the dependence of risk on the properties of specific threat Thr_p (intensity, location, etc.) under a given operating condition OC_j. In fact, the larger the intensity of a threat, the higher is the probability that a component fails (effect on probability) and the larger the set of components more prone to fail, i.e., the higher the impact on the system. Also the specific operating condition can affect both the severity and the probability of contingencies –given the same threat scenario-: for example, a lower meshing in network topology (e.g., due to the operation of substations with separate busbars) can favor cascading outages with amounts of disconnected load higher than in case of a more meshed topology (effect on impact); moreover, given the same ambient conditions in terms of wind speed and radiation, a higher current on an overhead line can increase the flashover probability due to contacts with trees (effect on probability).

TABLE IV
CHARACTERIZATION OF IMPACT INDICATORS

Impact	**Entities**	**Severity functions, $Imp_{j,ctg}$**	**Weights w_j**
Loss of load (LOL) [57]	Cascading paths	Loss of load at the end of cascading process	Path conditional probability
High current [6]	Branches	Continuous severity functions as in [6]	Branch rating, MVA
Low/High voltage [6]	Nodes	Continuous severity functions as in [6]	Nominal voltage, kV
Angle stability [59]	Generators	$\int_0^T \lvert \omega_j(\tau) - \omega_{COI}(\tau) \rvert d\tau$ ω_j = j-th rotor speed, rad/s ω_{COI}=Center of Inertia speed, rad/s, T = time window, s	Inertia constant on system base, s
Dyn over-voltage [59]	Nodes	$\int_0^T \max(0, v_j(\tau) - \bar{V}) d\tau$ v_j = node voltage, p.u. $\bar{V}$=max volt. thres., p.u.	Nominal voltage, kV
Dyn under-voltage [59]	Nodes	$\int_0^T \max(0, -v_j(\tau) + \underline{V}) d\tau$ $\underline{V}$=min volt. thres., p.u.	Nominal voltage, kV

Given the above statement, the risk indicator associated to a specific contingency *ctg* –henceforth called *Contingency Risk* CR_{ctg}– is given by (7).

$$CR_{ctg} = imp_{Thr_p}^{OC_j}(ctg) \times prob_{Thr_p}^{OC_j}(ctg) \tag{7}$$

where $imp_{Thr_p}^{OC_j}(ctg)$ and $prob_{Thr_p}^{OC_j}(ctg)$ are respectively the impact and the probability of the contingency (already defined in Section IV) as functions of operating conditions OC_j and threat Thr_p. The probabilistic modeling of threat Thr_p and vulnerabilities (described in Section III) and the combination of failure probabilities of components (see Section IV.B) provide term $prob_{Thr_p}^{OC_j}(ctg)$, while the simulation of power system response to contingency *ctg* through the cascading engine and time domain simulation provides term $imp_{Thr_p}^{OC_j}(ctg)$. In the following a shorter notation will be adopted replacing $imp_{Thr_p}^{OC_j}(ctg)$ with imp_{ctg} and $prob_{Thr_p}^{OC_j}(ctg)$ with $prob_{ctg}$ (already used in Section IV.B).

The AFTER approach provides both static and dynamic impact and risk indicators. Impact of contingency *ctg* is expressed as a weighted average of impact metrics $Imp_{j,ctg}$ on entities j, i.e., $Imp_{ctg} = \sum_j (Imp_{j,ctg} \times w_j) / \sum_j w_j$.

TABLE IV reports the weights and severity functions depending on the security problem. It's worth noticing that largest weights are associated to branches with higher ratings, to nodes with higher nominal voltages, and to generators with largest inertias: in fact, conventional engineering studies demonstrate that an overload on a highly rated branch may cause more severe problems to system security (like cascading outages, protection interventions, etc.) than the same entity of overload on a small rated branch. Similar considerations hold valid for the violations on node voltages, and for the deviations of generator speeds. One example of impact indicator is also the LOL (Loss of Load) metrics already mentioned in the description of cascading simulator in Section V.A. In this case, the severity function is the load lost at the end of j-th cascading path, while the weight consists in the conditional probability of the cascading path, calculated by recursively applying (6).

The general expression for system risk indicators SR is reported in (8).

$$SR = \sum_{ctg=1}^{N_{Thr_p}^{OC_j}} prob_{ctg} \cdot Imp_{ctg} \tag{8}$$

where $N_{Thr_p}^{OC_j}$ depends on specific threat Thr_p and operating conditions OC_j and represents the number of "dangerous" contingencies selected based on the two-stage contingency selection algorithm in Section IV.

It's worth noticing that the probability-based filtering in stage I accounts for the features of threat Thr_p from which the failure probabilities of the components are derived, while the risk-based stage II filters the contingencies on the basis of the estimated impact on the specific OC_j.

C. Influence Factors on Risk Assessment

Two main influence factors have been modeled:

- renewable and load forecast uncertainties; to evaluate their effect on operational risk, the AFTER tool gets the pdf's of the risk indicators by combining Point Estimate Method [60] and Third–order Polynomial Normal Transformation: simulation results and validation tests against Monte-Carlo sampling are reported in [61]. This modeling capability makes the methodology able to perform risk analyses on future power system states which are forecasted k hours in advance for operational planning studies. Simulations in Section VI are more focused on potential applications of the tool for security assessment analyses during the very short term operation of the power system on specific operating conditions: over a 10-15 minute future interval forecast uncertainties can be neglected and this functionality is not further discussed.
- uncertain response of automatic/manual defense systems due to ICT failures or operators' delays; the quasi static cascading engine includes the probabilistic models of: (a) Manual load shedding actions to relief congestions; (b) Automatic actions (anti-cascading load shedding; fast tripping of critical units) [62].

D. An Overview of the AFTER Risk Assessment Tool

Fig. 4 shows the architecture of the prototype for risk assessment, developed in MATLAB environment: each module is characterized by a specific letter put into brackets.

The upper modules of scenario generator (top part of the diagram) apply the probabilistic modeling to the threat and ICT/power system component vulnerability, determining the component failure probability [20]. Module C first applies the cumulative sum screening method, selecting the critical components (i.e., those which represent the fraction of "explained" total failure probability).

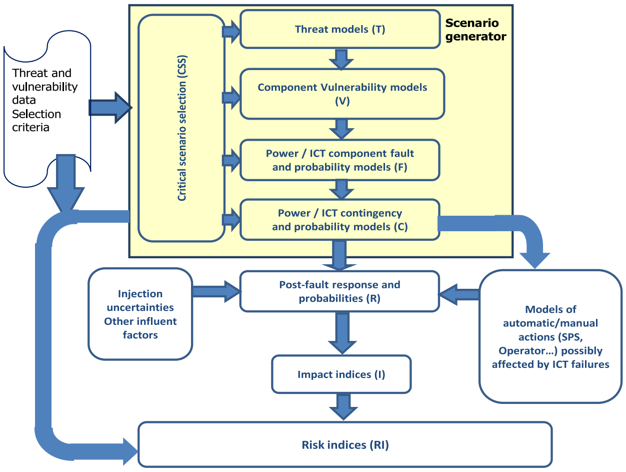

Scenario generator
Threat models (T)
Component Vulnerability models (V)
Power / ICT component fault and probability models (F)
Power / ICT contingency and probability models (C)
Critical scenario selection (CSS)
Threat and vulnerability data Selection criteria
Injection uncertainties Other influent factors
Post-fault response and probabilities (R)
Models of automatic/manual actions (SPS, Operator...) possibly affected by ICT failures
Impact indices (I)
Risk indices (RI)

Fig. 4. Architecture of the AFTER risk assessment tool for power and ICT risk assessment.

Thereafter, module C runs the enumeration technique to generate an exhaustive set of single and multiple (also dependent) contingencies, which are then screened using fast algorithms. The response of ICT/power system to contingencies is simulated using the time domain simulator and the cascading engine available in module R. This module can account for influencing factors like forecast uncertainties on loads and renewables and uncertain response of defence/control systems.

The impact of each contingency is computed in module I, and risk indicators are calculated by combining probability and impact in module RI. The final outcome consists of technical risk indicators to rank contingencies and track overall system security.

VI. Simulation Results and Discussion

This section presents results coming from extensive application of the tool to a real EHV grid, namely a portion of the Italian 220/400 kV system (about 80 nodes), and to the IEEE Reliability Test System [62]. The analysis is performed on the set of available models of threats, from natural threats (e.g., ice/snow storms) to human-related threats (sabotage). TABLE V reports the values adopted for the stress parameters of the models in Section III.

For each grid, two operating states are considered, respectively high and low demand. For each operating state and threat scenario, the tool extracts the set of dangerous contingencies. Standard values (used by the Italian TSO) are adopted for protection delay times. Risk indexes refer to a 10-minute interval: the paper focuses on the LOL risk index, as it is a relevant index to enhance power system reliability. Both contingency and system risk assessment functionalities are discussed in next subsections, including uncertainties related to protection responses and operators' behavior.

A. Contingency Risk Assessment

Contingency selection has been run adopting the two above-mentioned topological "ex-ante" impact metrics and several values of the selection parameters (the minimum ex-ante risk

TABLE V
CHARACTERIZATION OF THE 26 THREAT SCENARIOS

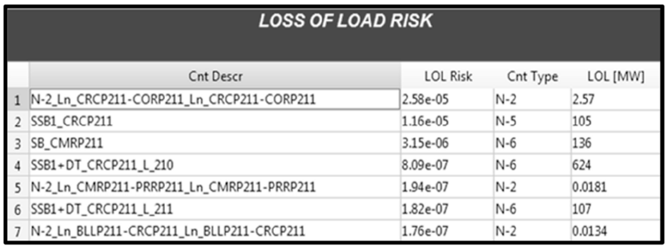
Short name	Stress variable	Scenario description
Snow storm 1	Wind speed peaks A1 A2 [m/s] Peak precipitation rate, PPR [mm/h] Initial precipitation level, IPL [mm]	A1 = 30; A2 = 35; PPR = 10; IPL = 10
Snow storm 2		A1 = 30; A2 = 35; PPR = 10; IPL = 30
Wind storm 1	Wind speed peaks A1 A2, [m/s]	A1 = 30; A2 = 35;
Wind storm 2		A1 = 40; A2 = 45;
Icing 1	PPR [mm/h] IPL [mm]	PPR = 5; IPL = 10
Icing 2		PPR = 5; IPL = 20
Pollution 1	Polluting agents concentration [mg/cm^2]	0.01 – mild pollution
Pollution 2		0.012 – moderate pollution
Pollution 3		0.015 – severe pollution
Lightning	Flash to ground density [# flashes/(km^2*h)]	Severe thunderstorm: 5.4*10^{-5} failures/15 min (per line span)
Earthquake 1	Peak ground acceleration [m/s^2]	Significant earthq.: magnitude 6
Earthquake 2		Catastrophic earthq.: magnitude 8
Landslide 1	Newmark displacement [m]	Landslides in earthquake 1
Landslide 2		Landslides in earthquake 2
Sabotage 1	Attack scenario probability [# attacks/week]	Activists against multiple targets; default physical protection
Sabotage 2		Professionals against multiple targets, default physical protection
Sabotage 3		Activists against multiple targets – high protection on OHL
Sabotage 4		Activists against multiple targets – low protection inside substations
Flood 1	Water level [m]	Catastrophic floods: max level 5 m. Elevated substation equipment
Flood 2		Severe floods: max level 4 m. Elevated substation equipment
Tree 1	Tree height [m]	Moderate trim. maintenance: expected tree height = 24m
Tree 2		Accurate trimming maintenance: expected tree height = 24m
Tree 3		Accurate trimming maintenance: expected tree height = 26m
Fire	Insulation temperature [°C]	Max Temp. 500°C in a substation
Aging 1	Air temperature [°C]	100 000 hours of operation
Aging 2		200 000 hours of operation

TABLE VI
CTG SET SIZE VS CTG SELECTION PARAMETERS – WIND STORM 1

	Fraction of explained failure probability					
	0.7		0.8		0.9	
	Ex-ante minimum risk threshold					
	10^{-10}	10^{-20}	10^{-10}	10^{-20}	10^{-10}	10^{-20}
Ctg order	**Contingency set size**					
N-1	6	6	8	8	9	9
N-2	15	15	28	28	36	36
N-k, k>2	26	70	28	246	28	425

threshold and the fraction of "explained" total failure probability). TABLE VI reports the number of contingencies to be analyzed for "wind storm 1" threat applied in the North West of the realistic EHV grid in the high load state, considering the net-ability metrics: for a 70% fraction, three double circuits are identified as critical (with a maximum failure probability of a circuit of $3.9 \cdot 10^{-4}/(10\text{ min})$). A 10^{-20} ex-ante risk threshold leads to 91 single and multiple common mode and dependent events, corresponding to 241 "dynamic" contingencies.

A high risk threshold limits the number of N-k contingencies to be analyzed, while the higher the fraction of explained failure probability the larger the number of selected N-1 and N-2. For the present scenario, a relatively high risk threshold permits to detect the multiple contingencies which most contribute to the total risk: in fact, for the 70% case, passing from 10^{-10} to 10^{-20} increases the number of selected N-k contingencies (from 26 to 70) with only a slight total LOL risk increase (+ 0.06%).



LOSS OF LOAD RISK

	Cnt Descr	LOL Risk	Cnt Type	LOL [MW]
1	N-2_Ln_CRCP211-CORP211_Ln_CRCP211-CORP211	2.58e-05	N-2	2.57
2	SSB1_CRCP211	1.16e-05	N-5	105
3	SB_CMRP211	3.15e-06	N-6	136
4	SSB1+DT_CRCP211_L_210	8.09e-07	N-6	624
5	N-2_Ln_CMRP211-PRRP211_Ln_CMRP211-PRRP211	1.94e-07	N-2	0.0181
6	SSB1+DT_CRCP211_L_211	1.82e-07	N-6	107
7	N-2_Ln_BLLP211-CRCP211_Ln_BLLP211-CRCP211	1.76e-07	N-2	0.0134

Fig. 5. Typical prototype outcome: a contingency ranking list.

Fig. 5 reports the LOL risk based ranking list of contingencies for "0.7 & 10^{-20}" case, in the typical tabular format for the outcome of the AFTER prototype. The headers of the columns of the output table refer to the identifier of the contingency ("CntDescr"), the risk of Loss of Load ("LOL Risk"), the category of contingency according to the number of outaged components ("Cnt Type"), and the severity of each contingency based on the amount of Loss of Load ("LOL [MW]").

The top contingencies are all multiple dependent contingencies (busbar faults with loss of half-busbars "SSB" or of entire busbar systems "SB", dependent failure on double circuit lines "DT"): the contribution of the most risky dependent N-2 (N-k) event is equal to 60% (30%) of total LOL risk: this demonstrates the relevance of multiple dependent contingencies in security assessment.

B. Effect of Threat Scenarios on System Risk

The second highlighted aspect is the ability of the tool to track the security of a power system operating state in case of changing weather/environmental phenomena, by monitoring global risk indicators over time. In particular, the global LOL risk indicator is assessed for the 26 threat scenarios described in TABLE V and applied to two operating states (autumn day peak load and night load) of the realistic EHV grid. Fig. 6 shows the global LOL risk indicators (expressed in dB, on basis 10^{-15}, due to the wide range of values).

Simulations point out the sensitivity to the threat magnitude (the minimum global risk increase from "mild" to "severe" threat is 14 dB).

Moreover, assessing the global LOL risk indicators allows quantifying the benefits of countermeasures adopted by TSOs: e.g., scenarios Sabotage 1 and Sabotage 3 compare different levels of physical security measures applied to transmission lines, while scenarios Tree1 and Tree2 compare two OHL (overhead line) pathway maintenance procedures. Simulations show that higher global risk values for some threats (pollution, flood, earthquake, landslide, tree contact, lightning and fire) are detected in the high load condition, while the other

TABLE VII
OUTCOMES OF CONTINGENCY SELECTION AND IMPACT ASSESSMENT FOR TWO THREAT SCENARIOS (WIND STORM 1 AND POLLUTION 1) AND TWO OC'S (HIGH AND LOW LOAD)

Threat	OC	Nr of critical components	Ctg category	Nr of ctgs per cat.	Contingency impact (lost MW)		Contingency probability		Contingency risk (expected lost MW in dB, basis = 10^{-15})		
					median	Up	Median	Up	median	Up	Fraction of total LOL risk, %
Wind Storm1	HL	6	N-1	6	$9.0 \cdot 10^{-4}$	$1.53 \cdot 10^{-2}$	$2.8918 \cdot 10^{-2}$	$2.8918 \cdot 10^{-2}$	84.18	97.17	28.4
			N-2	15	$9.4 \cdot 10^{-3}$	0.4191	$1.97 \cdot 10^{-4}$	$8.09 \cdot 10^{-3}$	58.91	96.52	7.3
			N-k	70	0.2625	629.01	$1.05 \cdot 10^{-6}$	$4.21 \cdot 10^{-6}$	46.90	100.70	64.3
Poltn1	HL	2	N-1	2	$1.8914 \cdot 10^{-2}$	$1.8914 \cdot 10^{-2}$	$5.67 \cdot 10^{-3}$	$5.67 \cdot 10^{-3}$	110.304	110.304	34.9
			N-2	1	0.448075	0.448075	$6.92 \cdot 10^{-4}$	$6.92 \cdot 10^{-4}$	114.916	114.916	50.5
			N-k	10	6.41349	121.285	$8.96 \cdot 10^{-8}$	$7.29 \cdot 10^{-7}$	76.7538	108.873	14.6
Wind Storm1	LL	6	N-1	6	$9.9 \cdot 10^{-3}$	11.1	$2.8918 \cdot 10^{-2}$	$2.8918 \cdot 10^{-2}$	95.29	124.94	98.5
			N-2	15	0.1997	24.42	$5.51 \cdot 10^{-7}$	$8.09 \cdot 10^{-3}$	72.82	108.82	1.4
			N-k	70	16.60	392.76	$1.05 \cdot 10^{-6}$	$4.21 \cdot 10^{-6}$	58.34	93.98	0.1
Poltn1	LL	2	N-1	2	$3.23 \cdot 10^{-4}$	$3.23 \cdot 10^{-4}$	$5.67 \cdot 10^{-3}$	$5.67 \cdot 10^{-3}$	92.6268	92.6268	39.6
			N-2	1	$7.378 \cdot 10^{-3}$	$7.378 \cdot 10^{-3}$	$6.92 \cdot 10^{-4}$	$6.92 \cdot 10^{-4}$	97.0814	97.0814	55.2
			N-k	10	0.189334	1.3378	$8.96 \cdot 10^{-8}$	$7.29 \cdot 10^{-7}$	64.8951	83.8411	5.2

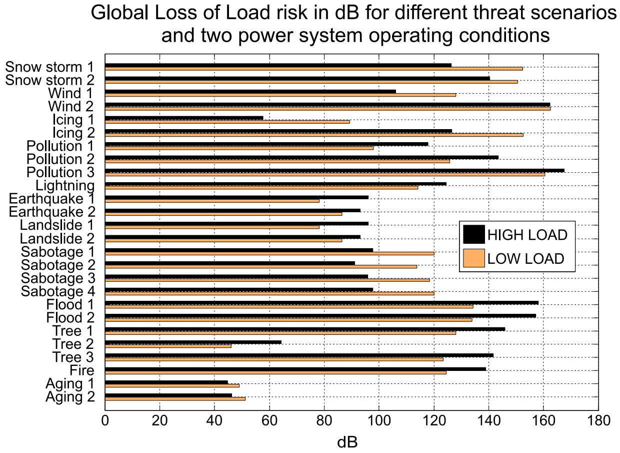


Fig. 6. Global LOL risk (in dB, with base level 10^{-15}) for high and low load operating conditions and for 26 different threat scenarios.

threats (icing, wind storm, snow storm, sabotage and aging) cause higher risk in the low load condition. In fact, threats have different ranges of influence: some threats are localized, hence they affect relatively few components; other threats are more widespread, hence it is more likely that several components are affected. Moreover, low and high load states differ for the meshing level of the grid: low load state is characterized by lower meshing level of the grid due to the operation of three 220/132 kV substations with separate half-busbars, hence a loss of load may occur even with a relatively low order contingency. To demonstrate this statement, TABLE VII reports some statistics (in particular, the number of critical components, the upper and median values for probability and LOL impact considering three contingency categories, N-1, N-2 and N-k, k>2) related to threat scenarios "wind storm 1" and "pollution 1" and to the two operating conditions under test. The same parameters for contingency selection are adopted in all cases (min ex-ante risk threshold $= 10^{-20}$ and fraction of explained failure probability $= 70\%$).

It's worth noticing that the number of critical components is different for the two threats: the same 6 critical components (specifically three 220 kV double circuits) are identified for the wind storm 1 scenario both in low and high load operating conditions, while only two critical components are identified in pollution 1 scenario: the larger geographical extent of wind storm 1 scenario determines a wider set of components with significant failure probabilities, and the cumulative sum screening method selects a larger set of components which explains 70% of the total failure probability. This demonstrates the differences in the interaction between threats and the grid.

The higher risk of wind storm 1 scenario in the low load scenario is due to the higher impact of N-1 contingencies which are also characterized by a higher probability of occurrence with respect to N-k, k >1 contingencies. TABLE VII shows that the median impact of a N-1 contingency passes from $9.0 \cdot 10^{-4}$ to $9.9 \cdot 10^{-3}$ from high load to low load operating condition: the contribution to total LOL risk coming from N-1 events passes from 28% to 98%. This is explained by the lower meshing level of the grid in the low load scenario: specific N-1 events in combination with possible hidden failures may cause more severe cascades in terms of lost load than in a more meshed grid configuration.

For pollution 1 scenario, the contributions of different contingency categories to total LOL risk do not change significantly from high load to low load scenario: the higher LOL risk in high load is due to larger impacts of N-1 events (0.0189 MW against $3.23 \cdot 10^{-4}$ MW) and of N-k events (median impact passes from 0.189 MW in low load *OC* to 6.41 MW in high load *OC*). Similar considerations hold valid for high current and low voltage risk indicators.

Overall, the not trivial simulation results show the importance of simulating current threats on the actual operating state. The noticeable contributions of multiple N-k dependent contingencies to the system risk for some threats in TABLE VII (e.g., wind storm 1 in high load *OC*) demonstrate that conventional security criterion based on credibility criteria (like N-1) underestimate the actual level of risk.

C. Effect of Relay Hidden Failures on System Risk

Assessing the effect of line protection hidden failures (i.e., inadvertent tripping) [58] on the risk of blackouts can provide

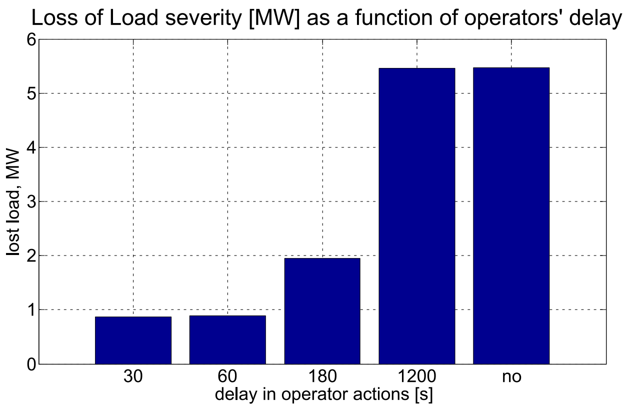


Fig. 7. The LOL severity for a specific contingency for different cases of operators' time delay in deploying control actions.

a valuable help both in operational planning and in maintenance policies. Threat scenario "pollution 1" is simulated for three values of hidden failure probabilities: 0% (no hidden failures), 1% and 5%. An increase in hidden failure probability from 0% to 5% brings a 239% increment of the LOL global risk: in fact, a higher hidden failure probability makes multiple inadvertent trippings (thus, cascading outages with loss of load) much probable also following frequent events, like N-1 contingencies, which greatly contribute to LOL risk, due to their high probability.

D. Effect of Operators' Actions on Contingency Risk

Given the high load operating condition of the IEEE RTS, subject to pollution scenario "pollution 1" and a 1% hidden failure probability, the tool is run for five case of operators' average delay times: 30 s, 60 s, 3 min., 20 min. and ∞ (i.e., no actions are deployed). The global LOL risk is reduced by 1% passing from "no action" to "30 s" case. The inclusion of operator actions may have little influence on the global LOL risk: in fact, operators' actions are immediately required only for very severe contingencies which usually little contribute to global risk, due to their very low probability (in most cases, allowable time for actions is not an issue). For some contingencies, the fast deployment of operators' action reduces the LOL severity. Fig. 7 reports the LOL severity index of one multiple busbar contingency for the five cases.

A mean value of operators' delay of 180 s reduces the LOL severity by 64% wrt "no action" scenario: identifying similar contingencies is crucial in operational planning. The knowledge of the time limits to assure the effectiveness of operators' actions helps improve system resilience and it is very valuable especially in case of extreme events or natural disasters where the quick and effective response by the operators is critical.

E. Effect of Delayed Intervention of Protection Schemes

Given "wind storm 1" threat on the high load state of the realistic EHV grid, the simulation goal is to quantify the risk increase due to malfunctioning of EHV line teleprotection, given the same contingency set. Thus, two cases are run: in case 1 a fault in zone 2 is cleared with an "accelerated" zone 1 tripping time of 140ms. Case 2 assumes that teleprotection does not work with a zone 2 tripping time of 400ms. The faults are applied at 10% from the 1st end of each line (i.e., system response depends on teleprotection status). TABLE VIII reports the variations of dynamic risk and impact indexes, respectively ΔR and ΔImp, caused by teleprotection malfunctioning, for groups of contingencies (N-1, N-2 and N-k, k>2).

TABLE VIII
RISK AND IMPACT VARIATIONS FOR TELEPROTECTION MALFUNCTIONING: RESULTS FOR N-1, N-2, AND N-k CONTINGENCIES

	Ctg type		
Δ indicators for impact and risk	**N-1**	**N-2**	**N-k**
mean/max $\Delta Imp_{angle\ instability}$	$5.92\cdot10^{-4}$/ $7.83\cdot10^{-4}$	$6.88\cdot10^{-4}$ / $7.33\cdot10^{-4}$	$7.64\cdot10^{-4}$/ 0.0058
$\Delta R_{angle\ instability}$, % wrt case 1	56.7	50.6	0.37
% of total $R_{angle\ instability}$: case 1 (2)	92.2 (94.3)	1.86 (1.83)	5.86 (3.84)
mean/max $\Delta Imp_{dyn.\ undervolt\ instability}$	$4.17\cdot10^{-4}$/ $6.21\cdot10^{-4}$	$5.47\cdot10^{-4}$/ $6.11\cdot10^{-4}$	$8.73\cdot10^{-4}$/ 0.0067
$\Delta R_{undervolt\ instability}$, % wrt case 1	3.1	2.7	0.02
% of total $R_{undervolt\ instability}$: case 1 (2)	91.8 (94.2)	2.01 (1.91)	6.24 (3.94)
mean/max $\Delta Imp_{dyn.\ overvolt\ instability}$	0.0085/ 0.014	0.0104/ 0.0128	0.0137/ 0.0507
$\Delta R_{overvolt.\ instability}$, % wrt case 1	252.7	232.7	0.99
% of total $R_{overvolt\ instability}$: case 1 (2)	87.5 (88.6)	1.68 (1.70)	10.8 (9.75)

For all dynamic security indicators, teleprotection malfunction mainly affects the impact of multiple N-k contingencies (highest mean impact increase), which also show large differences in impact increments: in fact, the impacts of some N-k multiple contingencies are not affected by teleprotection behaviour.

The largest N-k impact increment for angle instability problems refers to a multiple dependent event consisting of a fault on one bay of a substation close to a large power plant, with missing signal from primary protection and consequent intervention of back-up protections of all the branches connected to the half busbar with the faulty bay. In the present case, teleprotection malfunction mainly affects the risk of dynamic overvoltage which undergoes a drastic increase. Moreover, for all instability problems analyzed, the percentage contribution to total risk coming from multiple N-k contingencies is higher than N-2 contribution (thus not negligible, as assumed in conventional security analyses) and decreases when teleprotection does not work.

VII. CONCLUSION

The paper has presented an "extended" definition of risk, a comprehensive probabilistic risk based security assessment methodology and a tool suitable for operation and operational planning purposes. The proposed "all hazards" approach is able to adapt the set of single and multiple (also common mode and dependent) contingencies to be analyzed in security analyses, on the basis of short term evolution of the current threats, and to rank the contingencies using risk indicators. Extensive tests of the prototype on different operating states and threat scenarios demonstrate the importance of simulating actual threats in current power system operating conditions, in view of effective and comprehensive security analyses. The tool shows several potential advantages for the TSOs. First of all, the prototype helps operator improve the resilience of the power system: the "dynamic" selection of contingencies on the basis of the current environmental/weather threats allows operators to identify the most risky disruption scenarios in the near future (next few tens of minutes up to few hours), so that they can prepare suitable preventive/corrective actions to cope with them, should they actually occur. Moreover, the methodology has the following advantages over N-1 security assessment practice: first, contingency selection criterion is based on a risk concept and allows complementing conventional (N-1) security criteria, thus including also multiple common mode and dependent events, which may result in large disruptions. Secondly, the two-stage contingency screening process allows selecting a subset of most significant multiple contingencies, thus reducing the computational burden. Furthermore, the unified and flexible probabilistic framework based on an "extended" definition of risk allows modeling a large set of threats and component vulnerabilities in a coherent way; this represents a valuable step for a future exploitation of large sets of data provided by online monitoring systems at TSOs' control centers. The parameterization of hazard/vulnerability models lets the user perform sensitivity analyses to compare the effectiveness of different procedures (maintenance or physical security practices). The prototype can also help quantify the effect of hidden failures, operators' delays and delayed protection intervention on power system, providing also valuable contributions to assess power/ICT interdependencies.

References

[1] J.-P. Watson *et al.*, "Conceptual framework for developing resilience metrics for the electricity, oil, and gas sectors in the United States," Sandia Nat. Lab., Albuquerque, NM, USA, Tech. Rep. SAND2014-18019, Sep. 2014.

[2] I. Dobson, T. J. Overbye, and V. Vittal, "Engineering resilient cyber physical systems," Power Syst. Eng. Res. Center, Tempe, AZ, USA, Tech. Rep. 12-16, May 2012.

[3] U.K. Cabinet Office, "Keeping the country running: Natural hazards and infrastructure," Civil Contingencies Secretariat, London, U.K., Oct. 2011. [Online]. Available: https://www.gov.uk/government/uploads/system/uploads/system/uploads/attachment_data/file/61342/natural-hazards-infrastructure.pdf

[4] ENTSO-E, "Technical background and recommendations for defence plans in the continental Europe synchronous area," Subgroup Syst. Prot. Dyn., Brussels, Belgium, Jan. 2011. [Online]. Available: https://www.entsoe.eu/fileadmin/user_upload/_library/publications/entsoe/RG_SOC_CE/RG_CE_ENTSO-E_Defence_Plan_final_2011_public.pdf

[5] CIGRE, "Review of the current status of tools and techniques for risk-based and probabilistic planning in power systems," Working Group C4-601, TB no. 434, Oct. 2010.

[6] M. Ni, J. D. McCalley, V. Vittal, and T. Tayyib, "Online risk-based security assessment," *IEEE Trans. Power Syst.*, vol. 18, no. 1, pp. 258–265, Feb. 2003.

[7] D. E. Nordgård, K. Uhlen, B. H. Bakken, G. G. Løvås, and L. Voldhaug, "Implementation of a probabilistic security assessment tool for determination of power transfer limits," in *Proc. CIGRE Session*, Paris, France, Aug. 2002, pp. 1–6.

[8] M. A. Rios, D. S. Kirschen, D. Jayaweera, D. P. Nedic, and R. N. Allan, "Value of security: Modeling time-dependent phenomena and weather conditions," *IEEE Trans. Power Syst.*, vol. 17, no. 3, pp. 543–548, Aug. 2002.

[9] R. Preece and J. V. Milanovic, "Probabilistic risk assessment of rotor angle instability using fuzzy inference systems," *IEEE Trans. Power Syst.*, vol. 30, no. 4, pp. 1747–1757, Jul. 2015.

[10] C. Lemaitre and P. Panciatici, "iTesla: Innovative tools for electrical system security within large areas," in *Proc. IEEE PES Gen. Meeting*, Jul. 2014, pp. 1–2.

[11] NERC Standard TPL001-4, *Transmission System Planning Performance Requirements*, 2014.

[12] NERC Standard CIP-014-1, *Physical Security*, 2015.

[13] ENTSO-E, *Operational Handbook*, Mar. 2009.

[14] R. Baldick *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems," in *Proc. IEEE PES Gen. Meeting*, Pittsburgh, PA, USA, Jul. 2008, pp. 1–8.

[15] R. Billinton and G. Singh, "Application of adverse and extreme adverse weather: Modelling in transmission and distribution system reliability evaluation," *IEE Proc. Gener. Transm. Distrib.*, vol. 153, no. 1, pp. 115–120, Jan. 2006.

[16] M. H. J. Bollen, L. Wallin, T. Ohnstad, and L. Bertling, "On operational risk assessment in transmission systems—Weather impact and illustrative examples," in *Proc. 10th Int. Conf. Probabilist. Methods Appl. Power Syst. (PMAPS)*, Rincón, PR, USA, May 2008, pp. 1–6.

[17] Y. Liu, "Short-term operational reliability evaluation for power systems under extreme weather conditions," in *Proc. IEEE Eindhoven PowerTech*, Eindhoven, The Netherlands, Jul. 2015, pp. 1–5.

[18] M. Panteli and P. Mancarella, "Modeling and evaluating the resilience of critical electrical power infrastructure to extreme weather events," *IEEE Syst. J.*, to be published.

[19] E. Ciapessoni, "AFTER project objectives and results," presented at INNOGRID 2020+, Brussels, Belgium, Mar. 2014.

[20] UCTE (Union for the Co-Ordination of Transmission of Electricity). (2012). *Statistical Yearbook 2008*. [Online]. Available: http://www.entsoe.eu/

[21] E. Ciapessoni, D. Cirio, A. Pitto, G. Kjølle, and M. Sforna, "An integrated framework for power and ICT system risk-based security assessment," in *Proc. Powertech Conf. Grenoble*, Grenoble, France, Jun. 2013, pp. 1–6.

[22] A. V. Vecchia, "A unified approach to probabilistic risk assessments for earthquakes, floods, landslides, and volcanoes: Proceedings of multidisciplinary workshop held in Golden, CO, USA, in Nov. 16–17 1999," Tech. Rep. 2001-324, Golden, CO, USA, 2001.

[23] E. Ciapessoni *et al.*, "A probabilistic approach for operational risk assessment of power systems," in *Proc. CIGRE Session*, Paris, France, Aug. 2008.

[24] U. J. Minnaar, C. T. Gaunt, and F. Nicolls, "Characterisation of power system events on South African transmission power lines," *Elect. Power Syst. Res.*, vol. 88, pp. 25–32, Jul. 2012.

[25] CIGRE, "Big storm events what we have learned," Working Group B2.06, TB no. 344, Apr. 2008.

[26] A. H. Thieken, B. Merz, H. Kreibich, and H. Apel, "Methods for flood risk assessment: Concepts and challenges," in *Proc. Int. Workshop Flash Floods Urban Areas*, Muscat, Oman, Sep. 2006, pp. 1–12.

[27] E. Bostrom, J. Ahlberg, and L. Soder, "Modelling of ice storms and their impact applied to a part of the Swedish transmission network," in *Proc. Powertech Conf.*, Lausanne, Switzerland, Jul. 2007, pp. 1593–1598.

[28] E. Bon, R. Calisti, R. Fregonese, G. Gardini, and M. E. Gobbi, "Probabilistic assessment of electric power grids vulnerability under seismic action: A case study," *Struct. Infrastruct. Eng.*, vol. 9, no. 10, pp. 999–1018, 2013.

[29] W. Fu, J. D. McCalley, and V. Vittal, "Risk assessment for transformer loading," *IEEE Trans. Power Syst.*, vol. 16, no. 3, pp. 346–353, Aug. 2001.

[30] D. L. Wells and K. J. Coppersmith, "New empirical relationships among magnitude, rupture length, rupture width, rupture area, and surface displacement," *Bull. Seismol. Soc. America*, vol. 84, no. 4, pp. 974–1002, 1994.

[31] U.S. NRC, "The employment of empirical data and Bayesian methods in human reliability analysis: A feasibility study," Office of Nuclear Regul. Res., Washington, DC, USA, Tech. Rep. NUREG/CR-6949, Dec. 2007.

[32] A. Torres and P. Santos, "Bayesian networks and Monte Carlo simulations in the evaluation of the risk of terrorism for the Colombian electrical infrastructure," in *Proc. PMAPS Conf.*, Stockholm, Sweden, Jun. 2006, pp. 1–8.

[33] C. S. Engelbrecht, "A simplified statistical method for the qualification of insulators for polluted environments," Working Group CIGRE 33-01, 2002. [Online]. Available: http://clumb.free.fr/WG11/docs/public/33_01TF130104IWD.pdf

[34] *IEEE Guide for Direct Lightning Stroke Shielding of Substations*, IEEE Standard 998-1996, 1996.

[35] M. M. A. El Aziz, D. K. Ibrahim, and H. A. Kamel, "Estimation of the lifetime of the electrical components in distribution networks," *Online J. Electron. Elect. Eng.*, vol. 2, no. 3, pp. 269–273, 2010.

[36] GARPUR FP7 EU Project, "Current practices, drivers and barriers for new reliability standards," Deliverable 1.2, Jun. 2014.

[37] R. Barben, "Vulnerability assessment of electric power supply under extreme weather conditions," Ph.D. dissertation, Laboratoire Des Systèmes Énergétiques, École Polytechnique Fédérale de Lausanne, Lausanne, Switzerland, 2010.

[38] NORDEL. (2006). *Grid Disturbance and Fault Statistics*. [Online]. Available: http://www.nordel.org

[39] W. H. Bartley, "Analysis of transformer failures," in *Proc. 36th Annu. Conf. Int. Assoc. Eng. Insurers*, Stockholm, Sweden, 2003, pp. 1–5.

[40] M. Lauby, "State of reliability 2012," Rel. Assess. Perform. Anal. Group, North Amer. Elect. Rel. Corp., Atlanta, GA, USA, Tech. Rep., May 2012.

[41] *Nordic ENTSO-E Statistics*. (2012). [Online]. Available: https://www.entsoe.eu/

[42] *Guide for Improving the Lightning Performance of Transmission Lines*, IEEE Standard 1243-1997, 1997.

[43] CIGRE, "Polluted insulators: A review of current knowledge," Working Group TF 33.04.01, TB no. 158, 2000.

[44] P. Papakosta and D. Straub, "Effect of weather conditions, geography and human involvement on wildfire occurrence: A Bayesian network model," in *Proc. ICASP*, Zürich, Switzerland, 2011, pp. 1–8.

[45] S. D. Guikema, R. A. Davidson, and H. Liu, "Statistical models of the effects of tree trimming on power system outages," *IEEE Trans Power Del.*, vol. 21, no. 3, pp. 1549–1557, Jul. 2006.

[46] L. T. Rativa, "Évaluation du risque pour la sécurité des réseaux électrique face aux événements intentionnels," Ph.D. dissertation, Sciences de l'ing'enieur, Institut polytechnique de Grenoble, Grenoble, France, Apr. 2008.

[47] P. H. Corredor and M. E. Ruiz, "Against all odds," *IEEE Power Energy Mag.*, vol. 9, no. 2, pp. 59–66, Mar./Apr. 2011.

[48] I. J. Martinez-Moyano, E. Rich, S. H. Conrad, D. F. Andersen, and T. R. Stewart, "A behavioral theory of insider-threat risks: A system dynamics approach," *ACM Trans. Model. Comput. Simulat.*, vol. 18, no. 2, Apr. 2008, Art. ID 7.

[49] CIGRE, "Report on the second international survey on high voltage gas insulated substations (GIS) service experience," Working Group 23.02, TB no. 150, Feb. 2000.

[50] M. H. J. Bollen, "Literature search for reliability data of components in electric distribution networks," Dept. Elect. Eng., Eindhoven Univ. Technol., Eindhoven, The Netherlands, Tech. Rep. 93-E-276, Aug. 1993.

[51] O. Bahat, "Mitigation of transmission lines against bird hazards—The Israeli experience," in *Proc. EDM Int. Conf. Overhead Lines*, Fort Collins, CO, USA, Mar./Apr. 2010, pp. 1–14.

[52] H. P. Berg, N. Fritze, "Reliability of main transformers," *Rel. Theory Appl.*, vol. 2, no. 1, pp. 52–69, 2011.

[53] M. Bernardi, A. Borghetti, C. A. Nucci, and M. Paolone, "A statistical approach for estimating the correlation between lightning and faults in power distribution systems," in *Proc. PMAPS*, Stockholm, Sweden, 2006, pp. 1–7.

[54] P. Hines, S. Blumsack, E. C. Sanchez, and C. Barrows, "The topological and electrical structure of power grids," in *Proc. 43rd Hawaii Int. Conf. Syst. Sci.*, Honolulu, HI, USA, 2010, pp. 1–10.

[55] E. Bompard, E. Pons, and D. Wu, "Analysis of the structural vulnerability of the interconnected power grid of continental Europe with the integrated power system and unified power system based on extended topological approach," *Int. Trans. Elect. Energy Syst.*, vol. 23, no. 5, pp. 620–637, 2013.

[56] E. Ciapessoni, D. Cirio, and A. Pitto, "Cascadings in large power systems: Benchmarking static vs. time domain simulation," in *Proc. IEEE PES Gen. Meeting*, 2014, pp. 1–5.

[57] E. Ciapessoni, D. Cirio, S. Massucco, and A. Pitto, "A risk-based methodology for operational risk assessment and control of power systems," in *Proc. PSCC*, Stockholm, Sweden, Aug. 2011, pp. 1–7.

[58] X. Yu and C. Singh, "A practical approach for integrated power system vulnerability analysis with protection failures," *IEEE Trans. Power Syst.*, vol. 19, no. 4, pp. 1811–1820, Nov. 2004.

[59] E. Ciapessoni, D. Cirio, S. Massucco, A. Pitto, and F. Silvestro, "An innovative platform integrating deterministic and probabilistic tools for power system security assessment within a unified approach," in *Proc. Energy Conf.*, Florence, Italy, 2012, pp. 458–463.

[60] J. M. Morales and J. Perez-Ruiz, "Point estimate schemes to solve the probabilistic power flow," *IEEE Trans. Power Syst.*, vol. 22, no. 4, pp. 1594–1601, Nov. 2007.

[61] E. Ciapessoni, D. Cirio, and A. Pitto, "Effect of renewable and load uncertainties on the assessment of power system operational risk," in *Proc. PMAPS Conf.*, Durham, NC, USA, 2014, pp. 1–6.

[62] H. Vefsnmo *et al.*, "Risk assessment tool for operation: From threat models to risk indicators," in *Proc. Powertech Conf.*, Eindhoven, The Netherlands, 2015, pp. 1–6.

[63] P. M. Subcommittee, "IEEE reliability test system," *IEEE Trans. Power App. Syst.*, vol. PAS-98, no.6, pp. 2047–2054, Nov. 1979.

Emanuele Ciapessoni received the degree in physics and the Ph.D. degree in computer science from the University of Milan. He is currently the Leading Scientist with the Energy Systems Development Department, Ricerca sul Sistema Energetico S.p.A. (RSE, former ERSE and CESI RICERCA), and a Member of the Scientific Committee of RSE. His main research interests are in the fields of security assessment and control, distributed automation, risk evaluation, and risk mitigation of power systems. He has acted as an expert and was the WP leader and the Coordinator of several EU projects. He was the Coordinator of the EU Project AFTER. He is the Convenor of the Italian Electro-Technical Committee (TC) on Functional Safety, where he serves as an Italian Delegate of IEC TC 65 on Security and Safety of Control and Protection Systems.

Diego Cirio (SM'13) received the M.Sc. and Ph.D. degrees in electrical engineering from the University of Genoa, Italy, in 1999 and 2003, respectively. He is with Ricerca sul Sistema Energetico S.p.A. (RSE), Italy, where he leads the Grid Development and Security Research Group. He is scientifically responsible for RSE in EU and national research projects on the security of power systems with high renewable penetration and innovative technologies, such as BEST PATHS (operation of HVDC links and HVDC grid), iTESLA (online dynamic security assessment with uncertainties), AFTER (operational risk assessment), TWENTIES (offshore HVDC grid), and projects on ancillary services by RES. He acted as a Co-Operating Agent of the IEA Implementing Agreement ENARD Annex IV "Transmission Systems" and as the Task Leader in IEA ISGAN Annex 6 "T&D System Issues," where he currently acts as the national expert. He contributed to the CIGRE WG C4.601 on Power System Security Assessment.

Gerd Kjølle (SM'11) was born in Oslo, Norway, in 1958. She received the M.Sc. and Ph.D. degrees in electrical engineering from the Norwegian University of Science and Technology (NTNU, former NTH), in 1984 and 1996, respectively. She has been with SINTEF Energy Research since 1985, interrupted by a couple of periods with the Department of Electrical Power Engineering, NTNU. She is currently the Chief Scientist with the Department of Energy Systems, SINTEF Energy Research, and an Adjunct Professor with NTNU. Her research interests are in power system analysis and planning, reliability analysis, and risk and vulnerability analyses.

Stefano Massucco (M'80–SM'13) was born in Genoa, Italy, in 1954. From 1979 to 1987, he was at the Electrical Engineering Department, University of Genoa, CREL—the Electrical Research Center of ENEL (Italian Electricity Board), Milan, Italy, and ANSALDO S.p.A., Genoa. Since 1987, he has been an Associate Professor of Power Systems with the University of Pavia, and the Naval and Electrical Engineering Department, University of Genoa, since 1993, where he has been a Full Professor since 2000. His main research interests are in the field of electric energy systems and distributed generation modeling, control, and management; power systems analysis and simulation; and intelligent systems application to power systems. He has been scientifically responsible for several national research projects and EU projects dealing with distributed generation, energy saving, and smartgrids. He has authored over 180 scientific papers. He is a Member of the Italian Electrotechnical Committee and CIGRE Working Group 601 of Study Committee C4 for "Review of On-Line Dynamic Security Assessment Tools and Techniques."

Andrea Pitto (S'06–M'10) was born in Genoa, in 1981. He received the doctoral degree from the University of Genoa, Italy, in 2005, and the Ph.D. degree from the University of Genoa, in 2009, with a thesis on deterministic and probabilistic approaches to power system security assessment, both in electrical engineering. He was a Research Assistant with the Naval and Electrical Engineering Department, University of Genoa, from 2009 to 2010. He joined Ricerca sul Sistema Energetico S.p.A., in 2011. He is an Active Member of the IEEE Working Groups on Cascading Failures and Common Mode Dependent Outages. He is also a CIGRE Member and contributed to the CIGRE WG C4.601 on Power System Security Assessment. His areas of interest include probabilistic risk-based approaches to power system security assessment, and modeling and control of distributed generation and HVDC transmission systems.

Marino Sforna joined ENEL, the former Italian power company, as a Distribution Grid Designer, in 1982. From 1987 to 1997, he was with the Research and Development Department, working on renewables and AI applied to power system. From 1997 to 2001, he was the Deputy Manager of the Italian ISO Centers, Milan, and Venice. From 2002 to 2005, he was responsible for defense plans, restoration, protections, voltage, and frequency control at the Italian ISO. Since 2006, he has been with the Italian TSO, TERNA, where he is responsible for the Power System Risk Management Unit.