RESEARCH ARTICLE OPEN ACCESS

An Integrated Framework For Power And ICT System Risk-Based Security Assessment

Emanuele Ciapessoni*, Diego Cirio*, Andrea Pitto*, Marino Sforna**
*(Ricerca sul Sistema Energetico - RSE S.p.A., Milan, Italy)
** (TERNA, Italian Transmission System Operator, Milan, Italy)

ABSTRACT
Power system (PS) is exposed to natural and man-related threats which may affect the security of power supply, depending on the vulnerabilities of the system to the threats themselves as well as on the pre-fault operating conditions. Threats regard not only the power components, but also the Information and Communications Technology (ICT) systems involved in PS control and protection. The resulting picture is characterized by significant uncertainties, especially as far as high impact, low probability (HILP) events (typical causes of blackout events) are concerned. These considerations call for the adoption of novel techniques to perform more in-depth security analyses, able to identify the contributions of the different threats and vulnerabilities to the overall operational risk. The paper describes a probabilistic risk-based methodology, developed within the European Union (EU) research project AFTER (*A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration*), aiming to perform risk assessment (by means of *hazard, vulnerability,* and *impact* analysis) of the integrated power and ICT systems. Initial results of the approach are described with reference to a test system.

***Keywords* -** contingency analysis, power system security, risk assessment, power system dependences

I. INTRODUCTION

Electric power systems are vulnerable to different threats, from accidents and natural disasters, to deliberate acts of sabotage. Furthermore, system operation is critically dependent on the dependability and security of Information and Communication Technology (ICT) systems. As a matter of fact, these technologies have been extensively deployed by the power industry to manage the security of electrical power system. ICT systems have long supported monitoring and control by means of e.g. Supervisory Control and Data Acquisition (SCADA) systems. To deal with the increasing complexity of power system operation, due to market constraints, high power exchange over the interconnections, and, recently, the renewable power penetration, advanced apparatuses and systems are being installed worldwide. Examples are the Wide Area Monitoring Systems (WAMS). This trend is expected to continue in the future, especially in the perspective of the Smart Grid vision [1]-[3]. Protection and defense systems, including System Protection Schemes (SPS), also present a high degree of embedded expertise. They will also be encompassed among ICT systems in this work.

For these reasons, transmission system operators (TSOs) are increasingly concerned about whether the integrated Power & ICT system is adequately resilient with respect to failures, caused by different kinds of threats. The latter include equipment failures and/or subsystem malfunctions, natural events and disasters, negligence of the operators, malicious behavior such as deliberate acts of sabotage, criminal activity. All of these threats may result in multiple contingencies leading to extensive loss of electricity supply.

To manage critical scenarios, TSOs have to consider the interconnected electrical power system as a whole. National electrical power systems are in fact highly interconnected on a continental base. So, an outage originated in one area may propagate throughout the interconnection, spreading the disturbance to the close areas.

On this background, TSOs strongly need jointly-agreed practical methodologies to assess the operational risk in order to control risks and to guarantee an adequate security level for the interconnected network. These goals require a three-fold step forward:

1. Expressing security of supply in terms of risk, considering in particular how to manage wide area disturbances caused by multiple contingencies as an integration of conventional deterministic approaches to security (based on the N-1 criterion [4]) and convey a better insight into the risk.
2. A more integrated modeling of the Power and ICT subsystems to be considered in security assessment tools to evaluate the effects of their interdependencies on electricity supply. Several examples from recent blackouts support this

statement: the out of service of (both primary and backup) SCADA servers at FirstEnergy during North East US blackout in 2003 caused a loss of observability of the power system and a subsequent delay in deploying suitable corrective actions [5], which worsened the power system operation in the following minutes. Malfunction of protection systems due to wrong settings, inadequate logics, failures in actuators or measurement devices can delay the clearance of a fault or cause inadvertent tripping, reducing the stability of the power system, as demonstrated by the 2006 European blackout [6]. Wrong settings in defense systems (like SPS) can jeopardize the effectiveness of these measures in counteracting system disruption.

3. An extension of contingency analysis considering all types of hazards/threats, i.e., natural events, technical failures, human/operational errors and deliberate acts (e.g. sabotage), thus providing a more complete analysis of the causes for loss of supply.

As recently laid down by the European Commission in [7] one of the crucial objectives for the electricity networks is to identify methods and techniques to manage the security of the power system and to develop and validate advanced control systems, and monitoring techniques, to improve flexibility and security of the networks.

This paper presents the framework developed within the EU FP7 Project AFTER for the following goals: (1) classify the different (natural and man-related) threats; (2) perform risk assessment (including hazard, vulnerability, and impact analysis) of the integrated power and ICT systems, providing probabilistic models for the threats, for the vulnerability of components to the threats, as well as for the response of the integrated system to disturbances.

II. The AFTER project

The AFTER project, started in September 2011 and lasting 3 years, aims to increase the TSO capabilities in creating, monitoring and managing secure power system infrastructures, being able to survive large disturbances and to efficiently restore the supply after major disruptions [8].

These objectives have to be met by defining a framework – including methodologies, tools and techniques – able to:

1. Assess the risk, as hazard, vulnerability and impact analysis, of the interconnected and integrated electrical power and ICT systems [8].
2. Design and evaluate global defense and restoration plans.

Power system security must consider different kinds of vulnerabilities related to natural and man induced failures. Moreover, analyses aimed to check security of the power supply can no longer be limited to investigate the effects of power facilities outage and should include ICT failures within an integrated analysis. In order to assess risk, the following tasks are envisaged:

- identification and classification of threats and component vulnerabilities;
- probabilistic modeling of threats, component vulnerabilities and power system contingencies;
- simulation of the stochastic behavior of control, defense and protection systems in power systems affected by contingencies;
- definition and computation of risk indicators.

The following sections describe the mentioned classification of threats and the whole probabilistic framework for risk assessment.

III. Classification of threats affecting power and ICT components

A preliminary investigation of statistical yearbooks available at [9], as well as of the final reports of recent blackouts, allowed to identify the main causes of service and infrastructure disruptions and to propose a classification of the significant threats. Fig. 1 summarizes the contributions, as percentages of the total number of events, to the disturbances in the UCTE (now ENTSO-E Continental Europe - CE) grid, during 2008.

The AFTER project identifies two major layers, Power and ICT, interacting between each other, and it proposes a parallel and symmetric classification of the threats for both ICT components and power components.

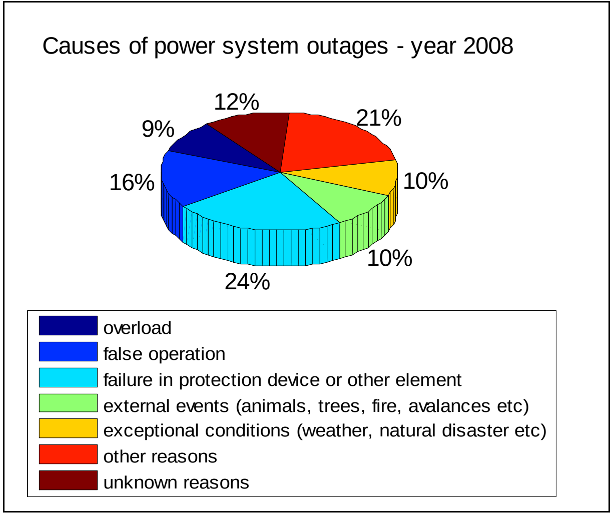

Fig. 1.Statistical analysis of the electric transmission faults in the UCTE Continental Europe (CE) area during 2008.

The proposed classification underlines the distinction between natural and man-related threats. A second dimension of the classification distinguishes between internal and external threats, respectively coming from inside or outside the boundaries of the system under study (including power and ICT components). Moreover, man-related actions can be intentional or not. Table I and Table II show the classification of some threats respectively to the power and ICT components. Notice that ICT threats may affect either the physical infrastructure or the logical level.

TABLE I – EXAMPLES OF THREATS TO POWER COMPONENTS

Power component threats	***External*** (Exogenous)	***Internal*** (Endogenous)
Natural	Lightning, fires, ice/snow storms, floods, solar storms	Component faults, strained operating conditions
Man-related	Unintentional damage by operating a crane; Sabotage, terrorism, outsider errors	Employee errors Malicious actions by unfaithful employees

TABLE II - EXAMPLES OF THREATS TO ICT COMPONENTS

ICT threats (Physical or Logical)	***External*** (Exogenous)	***Internal*** (Endogenous)
Natural	Ice and snow, floods, Fire and high temperature, solar storm	ICT component internal faults Data overflow
Man-related	Hacker, Sabotage, Malicious outsider	SW bugs, Employee errors, Malicious actions by unfaithful employees

A threat can affect different vulnerabilities of power-ICT components by activating stress variables (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.

Fig. 2 shows a schematic diagram linking threats, vulnerabilities, and contingencies. It is worth noticing that this scheme is valid for both ICT and power components.

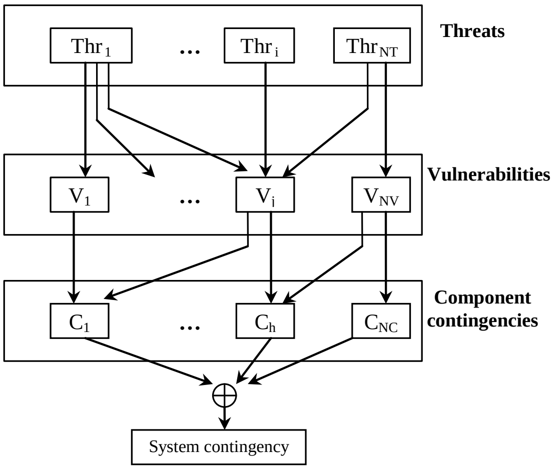

Fig. 2. Schematic diagram linking threats, vulnerabilities, and contingencies

IV. PROBABILISTIC FRAMEWORK FOR POWER SYSTEM CONTINGENCY MODELLING

Component failure can be described as the result of a threat exploiting one or more vulnerabilities of the component itself. Vulnerability can be characterized in probabilistic terms as the threat which can lead to a contingency with a probability P_V . Thus, vulnerability may be mathematically interpreted as the conditional probability of failure of a component given the occurrence of a specific threat. For example, a substation may not resist to a sabotage act, depending on the physical security measures adopted to protect it.

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.

1. General formulation

The general formulation to evaluate the failure probability of one component due to a specific threat derives from probabilistic vulnerability and hazard assessment analyses [10]. A model of the probability of failure of multiple components, due to the same threat, is herein proposed taking into account the cause-effect chains among different component functionalities. After that, the more general case with multiple components subjected to multiple threats is faced accounting for the possible dependencies among different threats. This formulation provides a general framework for probabilistic modeling of power and ICT system contingencies, to be used within risk approaches to security analysis.

The probability of failure P_F of a single component (either power or ICT) with vulnerability defined by a conditional probability function $P_V(t\,|\,\tau,s,x)$, at time *t*, subjected to a single threat with a {stress, time} multivariate probability density function (pdf) $p_{Thr}(\tau,s,x)$ can be expressed as:

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

where:

- $P_F(x,t)$ is the probability that the component, located in *x* - intact at initial time t_0 - fails within time instant *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 the vulnerability of the component is a function of time, due for instance to ageing or maintenance;
- $p_{Thr}(\tau,s,x)$ is the pdf of threat *Thr* applying stress *s* at location *x*, at time τ.

It is worth noticing that in (1) the term:

$$\left(\int_{S}P_V(t\,|\,\tau,s,x)\cdot p_{Thr}(\tau,s,x)ds\right)d\tau$$

represents the 'instantaneous' probability that component fails at time instant *t* due to threat *Thr*. 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*).

It is worth mentioning that influent factors (e.g. ambient temperature, humidity, etc.) can be included in the formulation by adding suitable terms in (1).

Discrete stress variables can also be treated in (1) by using Dirac impulses. "Distributed" components such as lines can be dealt with by extending the formulation to a set of discrete locations *x*.

2. Threat modeling

Multivariate distributions in (1) should be properly characterized according to the component and the threat under study. The selection of the most suitable models and the identification of parameters can be performed, on the basis of statistical data analysis. Historical data are enough for long term models (years ahead) adopted for expansion planning problems. However, characterizing medium term (some hours ahead) and short term (few tens of minutes ahead) models, used respectively for PS operational planning and operation, calls for additional data about the current or expected situation.

In particular, weather-related threat models may rely on information coming from weather forecast or real time weather monitoring services. In this way, the models can account for specific situations, as required in risk analyses aimed for operational planning or operation. As an example of probabilistic characterization of natural threats, Fig. 3 shows the contributions of different causes to electrical weather-induced disturbances for the 400 kV transmission lines in a portion of the Italian transmission system over years 1992-2002.

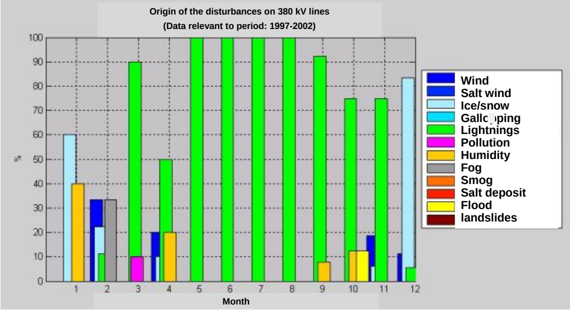

Fig. 3. Classification of different causes to electrical weather-induced disturbances, for 400 kV Italian transmission grid [11].

For some rare threats, accurate measurements may not available. These can be dealt with in a qualitative way, by associating high/low values according to whether the threat is known to be present or not present. It may be the case of animal-related threats (e.g. birds nesting on transmission lines, etc.), little documented in the literature (cf. [12]). On the other hand, "average" models of the threats can be devised (i.e. accounting for long term horizons), based on Bayesian networks. These models allow to effectively model the dependence of the threats on different factors like temperature, precipitation level, wind speed, etc. over such intervals. Bayesian networks can also be used to model the dependence of the probability of occurrence of fires on different factors like drought and air temperature.

Threats related to human behavior, both intentional and unintentional, are extremely difficult to represent. Qualitative information from experts can help to define such models. Human-related threats may derive, in a broad sense, from all fields of power and ICT system management, from planning (or design) of systems and components, to operation and maintenance. Procedures, use of instrumentation, training, availability of information, system feedback, workload, and stress, can all play a role. The characterization of human error probability distribution in (1) will exploit general methods, like the Performance Shaping Factors (PSF) [13], used to quantify the subjective assessment by experts.

Intentional attacks to power and ICT systems, including acts ranging from physical attacks of power infrastructures to cyber-attacks of SCADA systems, may be modeled using semi-Markov chains, attack trees and Bayesian networks. Fig. 4a) and b) represent two samples of the modeling solutions which will be considered in the AFTER project. The semi-Markov chain can represent the penetration into a computer system (a), and a Bayes network is suitable for physical attacks to the ICT and power infrastructures (b).

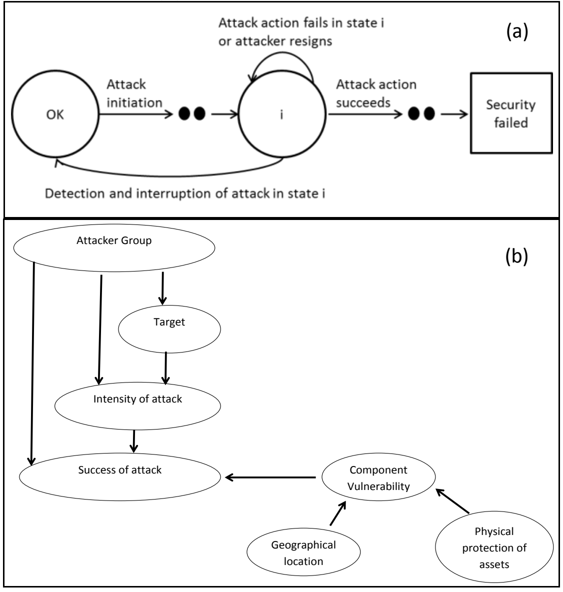

Fig. 4. Modelling intentional attacks: a) semi-Markov chain to model a computer penetration; b) Bayes network for a generic attack to the physical ICT and power infrastructure.

Logics adopted in the scheme of Fig. 4b) is explained below. A malicious attacker group chooses the target to strike on the basis of some considerations such as the availability of resources - like manpower, money, informers. The group expects some benefit from the attack: public shock, casualties, etc. The intensity of the attack, in terms of deployed human and material resources, depends on the target to be struck and on the belief of difficulty felt by attackers. The success of the attack depends on: the skill of the attackers to perform the action, the intensity of the attack and the vulnerability of the target itself. At last, the vulnerability of the target in turn depends on the geographical location and on the level of protection of the target itself. As for human error modeling, the intentional attack models can be tuned using mainly qualitative information coming from experts. An interesting property of Bayes network is that also logical and fuzzy discrete variables can be included into the model.

3. Vulnerability modeling

Each power and ICT component is subject to different threats which can exploit several of its vulnerabilities to damage it. Thus, in general, each component is characterized by a vulnerability function with respect to each threat. Some of these functions can be obtained from *ad hoc* tests, like voltage withstanding capacity curves for insulating materials, mechanical fragility curves, blast withstanding capacity curves. Other functions can be derived from qualitative information by experts, like the vulnerability of a SCADA system to cyber criminals.

It should be noticed that the vulnerability curves of the components also include ageing processes, which are modeled via suitable models like Arrhenius' model, or combined electric-thermal stress models [14].

4. Contingency

A contingency can be defined as the sequence of an initiating phenomenon or event, followed by the "immediate" response (fault-on response, in case the initiating phenomenon is a fault) of the protection and defence systems. Starting from the threat and component vulnerability models, a contingency can be characterized in probabilistic terms as the probability distribution of the time at which one or more components will fail.

Consideration of ICT systems is essential in contingency definition. In fact ICT systems play a crucial role in the fault response, which may be either "correct" or "not correct". In particular, protection systems have two major failure modes, respectively "failure to operate" when expected (lack of dependability), resulting in the intervention of backup protections, and "unnecessary trip" (lack of security), the latter also being referred to as "hidden failure". In both cases, the resulting contingency consists of the loss of more components with respect to the minimum set of faulty components. Moreover, ICT system malfunction may also play a role in the post-fault evolution, when more automatic actions or manual actions are involved.

V. PROBABILISTIC MODELING OF PS/ICT RESPONSE TO CONTINGENCIES

The assessment of the operational risk associated with a contingency requires the simulation contingency impact on the system. In turn, the response of the system to a contingency implies complex interactions among control, communication, protection and defense sub-systems, spanning over a broad range of time frames and covering wide geographical areas [15]. A contingency may eventually result into a cascading failure, defined by [16] as a sequence of dependent failures of individual components that successively weakens the power system.

1. Cascading engine within AFTER

The evaluation of cascading processes is central within the risk assessment method proposed in the AFTER project. Cascading failures are multifaceted because of the diversity of failures and of the interaction mechanisms they may trigger over different time scales. An exhaustive framework to assess cascading mechanisms is far from being achieved. An interesting overview of available methods, ranging from detailed simulations to network theory based models, is reported in [16].

Within the AFTER project, the starting point consists of a quasi-static approach implemented in the PRACTICE software tool [17], aimed to simulate at least the early stages of cascading triggered by system contingencies. This tool analyses several possible cascading paths, taking into account some sources of uncertainties in power system response, in particular (1) hidden failures in branches “exposed” by the fault and (2) uncertain settings in overcurrent protections.

The probability of hidden failure for an exposed branch (i.e. lines connected to the same nodes of the faulty line) depends on the branch current. A typical model is a linear one, starting from zero at 10% I_{nom} and reaching a maximum value p_0 (usually set to 1%) at I_{nom}. The uncertainty on protection relay settings is modeled via a normal distribution, with the tripping value of the relay state (normalized to 1 p.u.) as the mean, and a standard deviation σ_s (e.g. set to 2%). More details about the relevant probabilistic models can be found in [17].

The resulting approach is a probabilistic event tree, in which each state is defined by a state enumeration technique. The calculation of the probability of each cascading path over time t is based on the algorithm illustrated in Fig. 5.

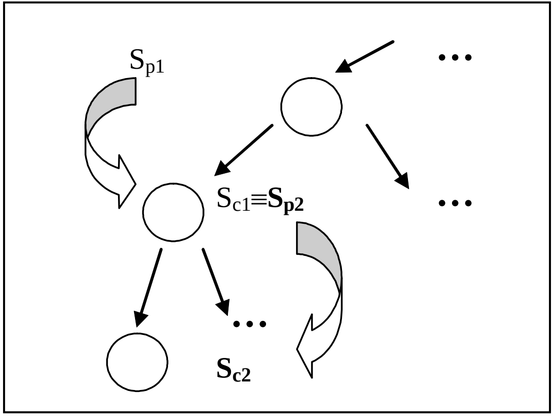

Fig. 5. Rationale of the algorithm to evaluate cascading path probability

At each cascading step, one can identify 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 contingency application.

The probability of having a certain child state S_c within time t, given a specific parent state S_p has occurred before time t, is given by (2).

$$P(t_{Sc} \le t, t_{Sp} < t) = \int_{t_0}^{t} P_{Sc}(t \mid \tau) \cdot p_{Sp}(\tau)\, d\tau \qquad (2)$$

where $p_{Sp}(\tau)$ is the probability density function of the time instant of occurrence of parent state S_p , and $P_{Sc}(t \mid \tau)$ is the conditional probability that state S_c occurs within time t given that parent state S_p has occurred at time instant τ.

In this way, each cascading path is characterized by a probability. Moreover, a loss of load can be associated to each path. Hence, the loss of load associated to the whole probabilistic event tree is defined in a probabilistic way, by properly combining these quantities (see [17] for details).

2. Risk indices calculation

Risk indices can be defined by combining contingency probability with contingency impact. To this regard, different impact metrics are defined, respectively:

- the loss of load at the end of the cascading process triggered by a contingency
- a function of the (over-) currents on the longitudinal elements just after fault clearing
- a function of the node (under- or over-) voltages immediately after the contingency.

Risk indices are defined as the expected value of the impact for the considered contingencies [17].

The cascading engine has an essential role in estimating the load lost at the end of each cascading path. It is based on a robust power flow program enhanced with steady-state models of frequency regulation (primary frequency control of generating units) and protection systems (branch overcurrent, minimum impedance for lines, minimum/maximum voltage for generators and loads, under- and over-frequency for generators). Moreover, manual load shedding (acting on interruptible loads, or on civil loads in emergency situations) as well as automatic load shedding (underfrequency load shedding and some logics of System Protection Schemes) are simulated. Operators’ behaviour is probabilistically represented in the prototype, by considering different levels of observability/controllability of the system, and time delays in deploying control actions. This leads to the development of more states in the probabilistic event tree.

In case of load-flow non-convergence, load reduction techniques (based on the evaluation of the nodal active residuals) are carried out in order to restore convergence. This may reflect either possible manual load shedding deployed by operators as emergency actions, or defence or protection systems which intervene when instability is approaching.
The cascading process goes on until there is no more significant violation, a complete blackout has been experienced, or a maximum number of steps has been reached.

VI. AFTER TOOL FOR POWER AND ICT RISK ASSESSMENT

The overall architecture of the tool for power and ICT risk assessment developed within AFTER is depicted in Fig. 6.

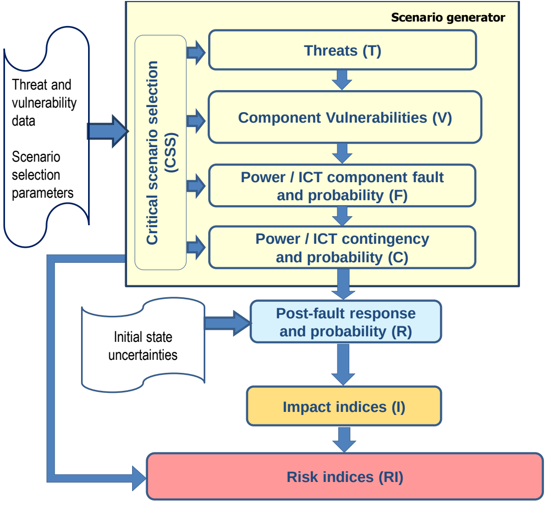
Scenario generator
Threat and vulnerability data
Scenario selection parameters
Critical scenario selection (CSS)
Threats (T)
Component Vulnerabilities (V)
Power / ICT component fault and probability (F)
Power / ICT contingency and probability (C)
Initial state uncertainties
Post-fault response and probability (R)
Impact indices (I)
Risk indices (RI)

Fig. 6. AFTER framework for power and ICT risk assessment

A threat evaluation module (block T in Fig. 6) considers both natural and man-related threats according to the abovementioned framework. After defining the vulnerabilities of components (or subsystems) to one or more threats (V), the component failure module (F) combines threat and vulnerability models. Dependencies among threats (multiple threats, common cause threats) are considered in order to provide system level evaluations. After that, the PS/ICT contingency identification module (C) elaborates the probabilistic model of a system contingency (defined as a combination of component failures) starting from single component failure probabilities: cause-effect chains among components and elements are investigated.

In particular, two important kinds of dependencies among components are modeled:

- *Geographical dependencies*: One threat can spread over a large portion of the grid, thus affecting different power and ICT components. For example, a snow storm can affect different transmission lines over a quite large area, or a flood can affect different substations.
- *Functional dependencies*: The failure of one component due to a threat may determine the failure of another component. Typical examples regard the contingencies resulting from protection malfunction, and from "double circuit line" (i.e. two lines on the same towers) failure. When protections do not operate correctly (either lack to operate or inadvertent operation), the resulting contingency is more severe than would be with correct protection behavior. As far as double circuit lines are concerned, if a lightning strikes a circuit of one such line, the other one may also experience short circuit. Similarly, the collapse of one circuit due to a snow storm may affect the second circuit.

The former kind of dependence is analysed by implementing a suitable geo-spatial model of the threat affecting the portion of the grid under study. The latter kind of dependence is tackled via a detailed description of substation configuration, as far as multiple contingencies due to protection malfunction are concerned. Advanced (in particular, copula-based [18]) probabilistic methods allow to model in detail the other functional dependencies.

The contingency module hence generates multiple contingency scenarios and their probabilities. A combinatorial explosion problem might arise here, due to the extremely large number of possible contingencies. To face this issue, the critical scenario selection function (CSS) (integrated in the previous modules) identifies a set of critical relevant contingencies, considering both PS and ICT failures.

In particular, to select the most plausible multiple dependent contingencies due to common threat, the *cumulative sum* screening method [19] is initially applied to identify the power and ICT components with the highest failure probabilities (henceforth defined as "critical components"). The outage of any combination of these components (with at most k_{max} outaged components) gives a first set of multiple contingencies considering geographical dependences among components. An additional set of multiple contingencies (caused by functional dependences) include possible contingencies affecting critical double circuits or power plants or the busbar systems of substations to which critical components are connected, taking into account substation configuration and possible malfunctions of primary protection systems.

In this way, a set of "N-k" contingencies is identified, associated to the failure of power and ICT components due to different threats and vulnerabilities.

The post-fault response module (R) evaluates the probabilistic system response to the contingencies, based on the cascading engine discussed above. As recalled in Fig. 6, by developing suitable techniques it may be possible to enhance the probabilistic evaluation of post-contingency evolution (post-fault and cascading), so as to account for the uncertainties in the initial system state e.g. due to forecast errors in renewable injections and loads. This development is currently under evaluation.

The impact evaluation module (I) calculates the severity indices (respectively based on current and voltage violations, and loss of load) associated to the contingency outcome.

Finally, the Risk indices calculation module (RI) provides global risk indicators of power system operation also accounting for ICT issues.

VII. CASE STUDY

A preliminary test of the AFTER risk assessment tool is run on the IEEE Reliability Test System [20]. The aim is to perform the risk assessment by focusing on one example of natural threats, i.e. lightnings, and analyzing the contingencies that result by considering ICT system malfunction.

1. Contingency modeling

Short term modeling of lightning-induced faults would be based on a real time monitoring system which provides information about imminent evolution of storms. In the present paper it is assumed that the electrical faults induced by lightning phenomena on Extra-High Voltage (EHV) branches are distributed according to an exponential distribution:

$$pdf(t) = \lambda \times e^{-\lambda \cdot t} \tag{3}$$

Fault rates λ in faults/(km*s) are listed in TABLE III. These parameter values are derived from statistical analyses of a large database referring to the Italian EHV transmission system [11].

TABLE III. RATE OF OCCURRENCE OF LIGHTNING-INDUCED FAULTS

Voltage level [kV]	**Failure rate □ [faults/(km*s)]**
380	$2.85*10^{-10}$
220	$3.51*10^{-10}$
132	$5.07*10^{-10}$

As a preliminary hypothesis, the same failure rate is applied to the busbar systems of the substations, assuming a standard length of busbars for each voltage level (20 m for 380 kV busbars and 30 m for 220 and 132 kV busbars). Similar failure rates have been found for other natural events (like snow) with reference to the Italian context. More refined models to model the initiating contingencies of both natural and human origin are being developed within the project.

In the present example, permanent faults are assumed to occur due to lightning, regarding:

- single branches (lines, transformers)
- busbar systems

The contingencies result from the following possible responses of primary and backup protections:

- "Correct" operation: protections identify the fault, send a tripping command to the involved circuit breakers which correctly operate. The fault is cleared by tripping the minimum number of components.
- Breaker failure (e.g. because it is stuck), followed by correct intervention of backup protections. In this case, more components are tripped to clear the fault. The resulting contingency is more severe than in the previous case.
- Failed operation of the bus differential protection (only in case of busbar fault): due to the malfunctioning it is not possible to isolate the faulty half-busbar, thus the subsequent intervention of backup protections lead to the loss of the entire busbar.

2. Results

A contingency set composed by single and multiple (also dependent) contingencies is applied to the components connected to bus 10 of the test system. The time interval of analysis, relevant for the evaluation of contingency probability, is 10 minutes. Risk of loss of load is expressed in dB (X_{dB} = 10 log(X/base) with base=10^{-20}). Thus, intervals on the y axis correspond to risk differences of orders of magnitude.

Fig. 7 compares the Loss Of Load (LOL) indicators for each contingency of the set, considering three different probabilities of hidden failures p_0 (0% -ideal case-, 1%, 5%).

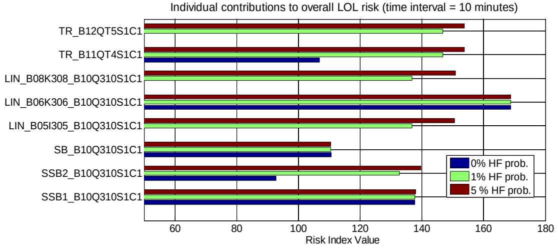

Fig. 7. Loss of load risk indicators for the set of contingencies under study (bus 10), for three different probabilities of hidden failure

TABLE **IV** shows the LOL risk indicators for the contingency set for the three p_0 values. It can be noticed that an increase of hidden failure probability by 5 times (from 1 to 5%, still a realistic value for such failures in a real world power system) causes a 10% increase of the risk of loss of load.

TABLE IV. LOL RISK VS. HIDDEN FAILURE PROBABILITY

Hidden failure probability, p_0, in %	**LOL risk, expected MW (Δt=10 minutes)**	**% Variation with respect to ideal case**
0 (ideal case)	7.37×10^{-4}	-
1	7.48×10^{-4}	+ 1.5
5	8.13×10^{-4}	+ 10.3

Fig. 8 shows the probability of having *x* steps of cascading along a cascading path related to contingency nr 6 (namely an N-1 line contingency affecting one HV line) in the next time interval of 10 minutes for the three values of hidden failure probability.

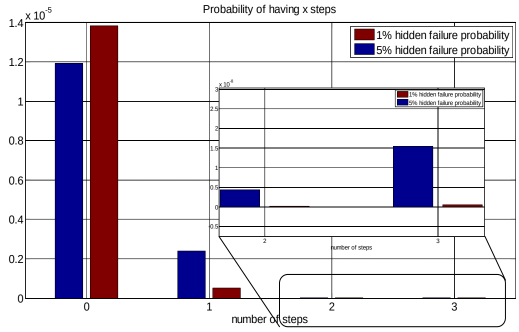

Fig. 8. Probability of having *x* steps of cascading within 10 minutes for the set of contingencies under study (bus 10), for three different probabilities of hidden failure

Case *x* = 0 corresponds to no cascading after the initiating contingency. It can be noticed that the higher p_0 the higher the probability of having longer cascading paths. In fact hidden failures cause a reduction of grid meshing, thus they weaken the grid configuration making longer cascading sequences more probable.

In particular, the increase of hidden failure probability from 1% to 5 % causes the probability of 3-step cascading (*x*=3) to pass from 7×10^{-10} to 1.7×10^{-8}.

Sensitivity investigations have been performed for parameter σ_s: as an illustrative example of the whole set of performed simulations, the increase in the standard deviation of the tripping probability distribution for overcurrent protections from 2% to 5% determines a 0.12% increase in the total LOL risk for the set of contingencies referred to bus 10. Thus, the influence of σ_s seems less significant with respect to p_0, at least within the considered ranges of σ_s.

VIII. CONCLUSION

This paper has presented the main features of a methodology and some preliminary applications of the relevant tool developed within the EU FP7 project AFTER to assess power system security in an operation and operational planning context using a risk-based approach. Further tests on a realistic model of the Italian EHV transmission system have been presented in [21]. The methodology fed by suitable probabilistic models for contingencies induced by both natural and man-related (also intentional) threats exploits a probabilistic simulator to assess ICT/PS system response to the abovementioned threats, taking into account possible interactions between ICT and power components. The evaluation of the impacts and of the probability of disturbances on the power and ICT system are fundamental to evaluate operational risk indicators like the risk of loss of load or the most likely number of branch trippings along a cascading path triggered by the disturbance.

The tool is being developed within AFTER project and it will be enriched with new probabilistic models, related to uncertain response of defense systems and of human behavior, as well as to the uncertain operating conditions of the PS/ICT systems (due to load changes, renewable intermittency).

IX. ACKNOWLEDGEMENTS

The research leading to these results has received funding from the European Union Seventh Framework Programme (FP7/2007-2013) under grant agreement n° 261788 and from the Research Fund for the Italian Electrical System under the Contract Agreement between ERSE and the Ministry of Economic Development - General Directorate for Energy and Mining Resources stipulated on July 29, 2009 in compliance with the Decree of March 19, 2009.

REFERENCES

[1] European Commission, “A European Strategic Energy Technology Plan - Towards a low carbon future”, Nov 2007

[2] ENTSO-E, EDSO, “The European Electricity Grid Initiative (EEGI) - Roadmap 2010-18 and Detailed Implementation Plan 2010-12”, May 25, 2010

[3] European Commission, Directorate-General for Research, “European SmartGrids Technology Platform - Vision and Strategy for Europe’s Electricity Networks of the Future”, 2006

[4] ENTSO-E, European Network of Transmission System Operators for Electricity, "Technical Background and Recommendations for Defence Plans in the Continental Europe Synchronous Area", January 31, 2011

[5] U.S.-Canada Power System Outage Task Force, "August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", Final report, April 2004

[6] UCTE (Union for the Co-ordination of Transmission of Electricity), "System Disturbance on 4 November 2006", Final report, January 2007

[7] "AFTER - A Framework for electrical power sysTems vulnerability identification, dEfense and Restoration", EU FP7 Project nr. 261788, Annex I, 2010

[8] European Commission, "Green paper on a European programme for critical infrastructure protection", EPCIP Green Paper COM(2005) 576, Nov 2005

[9] UCTE (Union for the Co-ordination of Transmission of Electricity), "Statistical Yearbook 2008", available at: www.entsoe.eu/

[10] A. V. Vecchia, "A Unified Approach To Probabilistic Risk Assessments for Earthquakes, Floods, Landslides, and Volcanoes", Proceedings of a Multidisciplinary Workshop, Golden, Colorado, Nov 16-17, 1999

[11] E. Ciapessoni, D. Cirio, E. Gaglioti, L. Tenti, S. Massucco, A. Pitto, "A Probabilistic Approach for Operational Risk Assessment of Power Systems", CIGRE Session, Paris, August 24-29, 2008, paper C4-114

[12] U. J. Minnaar, T. Gaunt, F. Nicolls, "Characterisation of Power System Events on South African Transmission Power Lines", Electric Power Systems Research, Elsevier, Feb 2012

[13] US Nuclear Regulatory Commission, "The Employment of Empirical Data and Bayesian Methods in Human Reliability Analysis: A Feasibility Study", Dec 2007

[14] M. Mamdouh Abd El Aziz, D. Khalil Ibrahim, H. Araby Kamel "Estimation of the Lifetime of Electrical Components in Distribution Networks", The Online Journal on Electronics and Electrical Engineering (OJEEE), July 2010

[15] P. Kundur, "Power System Stability and Control", McGraw-Hill, NY, 1994

[16] IEEE PES CAMS Task Force on Understanding, Prediction, Mitigation and Restoration of Cascading Failures, "Initial review of methods for cascading failure analysis in electric power transmission systems", IEEE PES General Meeting, Pittsburgh, PA, July 2008

[17] E. Ciapessoni, D. Cirio, S. Massucco, A. Pitto, "A Risk-based Methodology for Operational Risk Assessment and Control of Power Systems", 2011 PSCC Conference, Stockholm, Sweden, August 2011

[18] J. F. Mai, M. Scherer, "Simulating Copulas: Stochastic Models, Sampling Algorithms, and Applications", World Scientific, Vol. 4, 2012

[19] R. Barben, "Vulnerability Assessment of Electric Power Supply under Extreme Weather Conditions", Thesis, École Polytechnique Fédérale de Lausanne (EPFL), 2010

[20] Reliability Test System Task Force of the Application of Probability Methods Subcommittee, "IEEE Reliability Test System", IEEE Trans. on Power Apparatus and Systems, Vol. PAS-98, No.6 Nov./Dec. 1979

[21] E. Ciapessoni, D. Cirio, A. Pitto, "Cascading simulation techniques in Europe: the PRACTICE experience" (presentation), 2013 IEEE PES General Meeting, Vancouver, BC, Canada, July 21-25, 2013