Whither probabilistic security management for real-time operation of power systems ?

Efthymios Karangelos*, Patrick Panciatici†, Louis Wehenkel*

*University of Liège, Belgium †RTE-DMA, France

Abstract

This paper investigates the stakes of introducing probabilistic approaches for the management of power system's security. In real-time operation, the aim is to arbitrate in a rational way between preventive and corrective control, while taking into account i) the prior probabilities of contingencies, ii) the possible failure modes of corrective control actions, iii) the socio-economic consequences of service interruptions. This work is a first step towards the construction of a globally coherent decision making framework for security management from long-term system expansion, via mid-term asset management, towards short-term operation planning and real-time operation.

Nomenclature

Indices:

b	Index of corrective control behaviors.
c	Index of contingencies.
d	Index of demands.
g	Index of generating units.
ℓ	Index of transmission lines.
n	Index of nodes.

Sets:

$\mathcal{D}_n$	Set of demands connected at node n.
$\mathcal{G}_n$	Set of generating units connected at node n.
$\mathcal{N}_b$	Set of corrective control behaviors.
$\mathcal{N}_c$	Set of contingencies.
$\mathcal{N}_d$	Set of demands.
$\mathcal{N}_g$	Set of generating units.
$\mathcal{N}_\ell$	Set of transmission lines.
$\mathcal{N}_n$	Set of nodes.

Parameters:

c_g	Marginal generation cost of generating unit g.
c_g^r	Marginal corrective re-dispatch cost of generating unit g.
P_g^{max}	Capacity of generating unit g.
P_g^{min}	Minimum stable generation of unit g.
P_g^-	Ramp-down limit of generating unit g.
P_g^+	Ramp-up limit of generating unit g.
ΔP_g^e	Emergency ramp-down limit of generating unit g.
w_g	Disconnection severity coefficient of generating unit g.
P_d^0	Load of demand d.
v_d	Value of lost load of demand d.
f_ℓ^{max}	Capacity of transmission line ℓ.
X_ℓ	Reactance of transmission line ℓ.
$\beta_{n,\ell}$	Element of the flow incidence matrix, taking a value of one if node n is the sending node of line ℓ, a value of minus one if node n is the receiving node of line ℓ, and a zero value otherwise.
π_c	Probability of occurrence of contingency c.
π_b	Probability of realization of corrective control behavior b.
s_{max}	Severity threshold.
a_i^c	Binary parameter taking a zero value if component $\{i \in \mathcal{N}_g \cup \mathcal{N}_\ell\}$ is unavailable under contingency $c \geq 1$.
τ_c	Binary parameter taking a value of one if contingency $c \geq 1$ concerns the failure of a generating unit.
M	A large constant.

Continuous Variables:

P_g^0	Power output of generating unit g under the pre-contingency state.
P_g^c	Corrective control schedule of generating unit g under contingency $c \geq 1$.
$\hat{P}_g^c(b)$	Power output of generating unit g at the terminal state following the occurrence of contingency $c \geq 1$, the realization of corrective control behavior b and the application of emergency control actions.

f_ℓ^0 — Power flowing through transmission line ℓ under the pre-contingency state.

$f_\ell^c(b)$ — Power flowing through transmission line ℓ under contingency $c \geq 1$ and corrective control behavior b.

$\hat{f}_\ell^c(b)$ — Power flowing through transmission line ℓ at the terminal state following the occurrence of contingency $c \geq 1$, the realization of corrective control behavior b and the application of emergency control actions.

$\hat{P}_d^c(b)$ — Load of demand d at the terminal state following the occurrence of contingency $c \geq 1$, the realization of corrective control behavior b and the application of emergency control actions.

θ_n^0 — Voltage angle at node n under the pre-contingency state.

$\theta_n^c(b)$ — Voltage angle at node n under contingency $c \geq 1$ and corrective control behavior b.

$\hat{\theta}_n^c(b)$ — Voltage angle at node n at the terminal state following the occurrence of contingency $c \geq 1$, the realization of corrective control behavior b and the application of emergency control actions.

$\delta_n^c(b)$ — Slackness on the power balance at node n under contingency $c \geq 1$ and corrective control behavior b.

$s^c(b)$ — Severity of the terminal state following the occurrence of contingency $c \geq 1$, the realization of corrective control behavior b and the application of emergency control actions.

Note: All continuous variables are non-negative with the exception of the line flow variables, voltage angle variables, and slack variable $\delta_n^c(b)$.

Binary Variables:

$\lambda_\ell^c(b)$ — Binary variable, taking a value of one if there is an overload in transmission line ℓ under contingency $c \geq 1$ and corrective control behavior $b \in N_b$.

$p_\ell^c(b)$ — Binary variable, taking a value of one only if the flow of transmission line ℓ is positive under contingency $c \geq 1$ and corrective control behavior $b \in N_b$.

$\gamma^c(b)$ — Binary variable, taking a value of one if the severity of the terminal state following the occurrence of contingency $c \geq 1$ and the realization of corrective control behavior $b \in \mathcal{N}_b$ is greater than the respective threshold.

$y_g^c(b)$ — Binary variable taking a value of one if generating unit g has to be disconnected under contingency $c \geq 1$ and corrective control behavior b.

I. Introduction

In today's power systems security management practice, the $N-1$ criterion is used (with slightly different interpretations in different control areas) to express an acceptable level of security. This fundamental criterion is consistently considered throughout overlapping decision horizons, ranging from long-term system expansion, via mid-term asset management, to short-term operation planning and real-time operation.

The ageing of the power system infrastructure and the increasing penetration of renewable and dispersed generation presently induce new threats to the system security. At the same time, the potential incorporation of emerging smart grid technologies poses as a new opportunity. Such developments call more and more for the explicit consideration of uncertainties through the development of alternative security criteria and more effective decision making frameworks [1], [2], [3], [4], [5], [6].

The idea of framing power systems security management in a probabilistic paradigm is appealing but not new. Since the 1970's, several proposals to formulate probabilistic variants of the problem and to develop solutions via tractable algorithmic approximations have been presented (see, *e.g.* [7], [8], [9], [10], [11]). Yet, none of these proposals has gained acceptance by TSOs and Regulators, as the practical difficulties for using probabilistic methods instead of the $N-1$ criterion are multifold: i) data quality issues, ii) computational complexity limitations, iii) the allocation of security provision and service interruption costs among control areas and end-users, iv) methodological limitations in the assessment of the social benefit of moving away from the $N-1$ criterion.

Since security management is a multi-stage/multi-actor optimisation problem (covering the different time-horizons from long-term to short-term and ranging over multiple subsystems coupled horizontally or vertically) it is necessary to be able to appraise (and then be able to adapt to) any suggested change in the decision making strategy adopted in any one of these sub-problems.

A. Proposal

In the present paper we focus on the latest decision horizon, namely real-time operation. In this context, we investigate the stakes of introducing a probabilistic approach to arbitrate between preventive and corrective control alternatives.

Reliance on corrective control measures is inevitably growing in response to the aforementioned increasing stress and uncertainty in power system security management. Yet, as with every system component, the operation of corrective control is also characterized by a certain degree of uncertainty. The fact that corrective control may fail to operate as anticipated implies that the use of this resource does not fully nullify the possibility of realizing undesirable

system states resulting in unacceptable service disruption levels. Explicitly acknowledging this feature, we propose to account not only for the operational cost of corrective control but also for the societal costs arising from the corrective control potential behavior modes.

To that end, we introduce a decision making approach on the basis of the socio-economic cost induced by a security management strategy. The socio-economic cost of a security management strategy comprises both of operational costs incurred by the TSO as well as of societal costs associated with the potential service disruption to the system users. In order to encapsulate the conceptual difference between the former and the latter, we consider the avoidance of potentially severe societal costs as an integral task of power system security management. We thus frame a probabilistic security management concerning both economy and risk [12], through the following interrelated objectives:

- **Primary Objective:** Avoid with a certain confidence the potential realization of extremely severe societal cost levels.

- **Secondary Objective:** Minimize the expectation of the socio-economic costs of security under all credible system states.

B. Paper Organization

We begin by presenting in section II the general form of the problem in question and discussing the main modeling issues that should be addressed. In the final part of this section, we also introduce a set of approximations adopted to develop a tractable algorithmic approach for the purposes of this paper. Based on such approximations, in section III we establish the detailed mathematical formulation of the considered problem as a Mixed-Integer Linear Programming (MILP) problem. In section IV, we demonstrate the properties of this proposal through a single-area academic test system and assess its effects on a comparative basis, with respect to the well-known N-1 approach. In section V we consider an alternative set of case studies concerning a system with two control areas. We conclude in section VI by summarizing the key findings of this work and discussing in detail the main challenges toward the adoption of probablistic power system security management practices.

II. Security management in real-time operation

In the present section we establish the general form of the proposed probabilistic real-time security management approach. Furthermore, we highlight the key modeling challenges and introduce a set of approximations employed in this paper for the sake of tractability.[1]

---

[1]For notational simplicity, but without loss in generality, we assume that all uncertainties range over a finite number of possibilities.
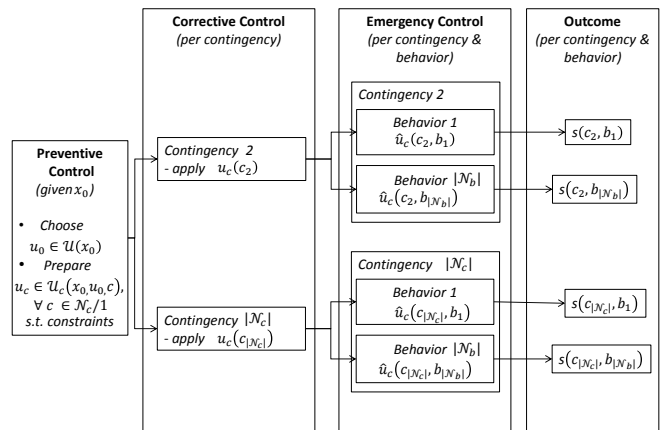

Fig. 1. Decision making stages and outcomes

A. Modelling the set of possible scenarios

Let us denote by $\mathcal{N}_c$ the set of possible contingencies, by x_0 the current operating state of an interconnected system, by $\mathcal{U}_0(x_0)$ the space of possible preventive control actions accessible to a TSO operating one area of this system, and for any pair $(u_0, c) \in \mathcal{U}_0(x_0) \times \mathcal{N}_c$ by $\mathcal{U}_c(x_0, u_0, c)$ the space of possible corrective control actions accessible to it. (Please, preview Figure 1, before reading this section.)

We assume that the set of contingencies $\mathcal{N}_c$ describes in a mutually exclusive and exhaustive way the events that may happen during the next period of time T, and we denote by $\pi_c \in [0; 1]$ their elementary probabilities, with $\sum_{c \in \mathcal{N}_c} \pi_c = 1$.[2]

The job of the TSO is to choose a joint decision strategy u combining a preventive control choice $u_0 \in \mathcal{U}_0(x_0)$ and a set of corrective control choices $\{u_c \in \mathcal{U}_c(x_0, u_0, c)\}_{c \in \mathcal{N}_c}$. We denote by $\mathcal{U}(x_0)$ the space of all joint preventive-corrective control strategies accessible to the TSO. Once a joint strategy $u \in \mathcal{U}(x_0)$ is chosen, the TSO applies its preventive decision u_0 and then waits for the potential realization of a contingency c to apply the corresponding corrective control u_c.

Since corrective control is carried out under time pressure, and since the system state may change in an unpredictable way between the moment when a control action has been selected and the moment it is applied, we do not assume that the physical effect of the control strategy is fully predictable [13]. Rather, we assume that for each four-tuple (x_0, u_0, c, u_c) there is a set of possible post-contingency behaviors $\mathcal{N}_b(x_0, u_0, c, u_c)$ that may occur; for each possible behavior $b \in \mathcal{N}_b(x_0, u_0, c, u_c)$ we denote by $\pi_b(b|x_0, u_0, c, u_c) \in [0; 1]$ its probability of occurrence, with $\sum_{b \in \mathcal{N}_b(x_0, u_0, c, u_c)} \pi_b(b|x_0, u_0, c, u_c) = 1$.[3]

---

[2]The set $\mathcal{N}_c$ will thus in general contain also a pseudo-contingency which corresponds to the case where no actual contingency is triggered during the interval T.

[3]In the most simple case, the set $\mathcal{N}_b$ would be composed of only two elements, one modelling perfect operation of corrective control, and one modelling complete failure of corrective control.

B. Security level induced by a decision strategy

We assume that the TSO can evaluate the impact of its decision strategies on power system security by computing a *severity function* $s(x_0, u_0, c, u_c, b) \in \mathbb{R}^+$. Such a severity function would be computed from the system dynamics induced by the choice of the preventive control action u_0, the occurrence of the contingency c, the application of the corrective control action u_c, and the realization of the post-contingency behavior b. This function would serve as a measure of the societal cost of the service disruptions realized by the end-users of its own control area.[4]

For a given x_0 and a fixed strategy u, s is thus a random variable. Let us define the two following quantities to describe its dependence on the choice of u:[5]

$$\mathbb{P}_{s \leq s'|x_0,u}(u) = \sum_{c \in \mathcal{N}_c} \pi_c \sum_{b \in \mathcal{N}_b} \pi_b(b|x_0, u_0, c, u_c) 1(s \leq s'), \quad (1)$$

which is the probability that the severity level s is smaller or equal than the threshold s', given the strategy u, and

$$\mathbb{E}_{s|x_0,u}(u) = \sum_{c \in \mathcal{N}_c} \pi_c \sum_{b \in \mathcal{N}_b} \pi_b(b|x_0, u_0, c, u_c) s, \quad (2)$$

which is the expected severity level induced by u.

C. Formulating the optimal decision making problem

As already stated, we propose to formulate the task of the TSO in real-time operation security management through a combination of two objectives:

- **Primary objective:** avoid service interruptions of large severity to a certain possible extent. We model this objective by the choice of: i) a maximal severity level $s_{\max}$ to avoid and ii) a small risk ϵ of not being able to avoid it, i.e. in the form of the chance constraint:

$$\mathbb{P}_{s \leq s_{\max}|x_0,u}(u) \geq 1 - \epsilon. \quad (3)$$

- **Secondary objective:** minimise a cost-function which combines the direct operating costs incurred by the strategy and the societal costs measured by the expectation of the severity function:

$$
\begin{aligned}
C(x_0, u) &= C_0(x_0, u_0) + \sum_{c \in \mathcal{N}_c} \pi_c C_c(x_0, u_0, c, u_c) \\
&\quad + \mathbb{E}_{s|x_0,u}(u).
\end{aligned} \quad (4)
$$

[4]We note that the computation of such a severity function may require very detailed dynamic simulations to identify the joint physical effect of the TSO's actions and post-contingency behaviors. Moreover, in order to express the physical quantities characterizing the resulting terminal state of the system in monetary terms, various assumptions about the durations and costs of service interruptions would be required.

[5]The operator $1(s \leq s')$ takes a value of one if $s \leq s'$, and otherwise takes a value of zero.

The real-time decision making problem (**RTP**) hence is compactly expressed in the following way:[6]

> **RTP** : Compute: $u^*(x_0) \in \arg\min_u C(x_0, u)$ (5)
>
> subject to: $\begin{cases} u \in \mathcal{U}(x_0), \\ \mathbb{P}_{s \leq s_{\max}|x_0,u}(u) \geq 1 - \epsilon. \end{cases}$ (6)

D. Scalable approximation strategies

In large-scale power systems, the quantities $C(x_0, u)$ and $\mathbb{P}_{s \leq s_{\max}|x_0,u}(u)$ used in our formulation can't be calculated exactly, even for a single "given" strategy u (and even if we consider that $\mathcal{N}_c$ and $\mathcal{N}_b$ are finite sets). Hence the exact solution of the **RTP** optimisation problem is certainly out of reach in realistic conditions.

As a starting point in the direction of providing tractable solutions to this problem, in the present paper we adopt the following approximations:

(i) We express all network constraints under the DC power flow model [14]. On this basis, we consider the pre-contingency scheduling of the generating units as the preventive control action available to the TSO. Following the occurrence of any contingency $c \geq 1$, the set of available control actions corresponds to the re-dispatch of the generating units that were operational in the pre-contingency state.

(ii) We restrict to considering that the set $\mathcal{N}_b$ comprises solely of two elements, corresponding to the working and failing behaviors of corrective control respectively. Under the latter, corrective control would be completely ineffectual. In such a case, all controllable resources (*i.e.* dispatchable generating units) would remain at their preventive operating points.

(iii) Following from approximation (ii), the realization of the corrective control failing behavior under the case of a generating unit outage would result in a net energy deficit. In such a case, we seek for a terminal system state, as in approximation (v), by considering that the transmission network remains intact.

(iv) Also following from approximation (ii), the realization of the corrective control failing behavior under the case of a line outage may result in overloading additional network branches. In such a case, prior to identifying the terminal system state we model the removal of such branches from service.

(v) Under both line and generating unit outages, we seek for a feasible terminal system state following the realization of corrective control behavior $b \in \mathcal{N}_b$ by means of the following emergency control actions:

   – Shedding load across any network node.

[6]In this formulation all typical OPF constraints, such as static load-flow equations, control feasibility ranges, etc., are incorporated in the description of the set of admissible joint strategies $\mathcal{U}(x_0)$.

- Allowing generating units to ramp-down within a limited range in response to the load shedding. We note that in the case that the corrective control failing behavior was realized, this limited range is applicable with respect to the preventive operating points of all generating units that were not affected by the initiating contingency.
- Imposing that in case a generating unit cannot operate within the aforementioned limited range it would be disconnected from the network.

(vi) Following the application of the emergency control actions listed in approximation (v) we adopt a linear severity function to express the societal cost of the service disruption. In this function we employ a load-specific per unit free (in $\text{\euro}/MWh$) to denote the cost incurred by any electricity consumer subject to a service interruption. With regard to generating units, we do not consider any emergency control cost in the event that they are merely forced to ramp-down within the aforementioned limited range. We recall that function (4) explicitly accounts for the costs of the preventive and corrective dispatch under every credible system state. As such, we restrict to considering a unit specific fixed fee (in $\text{\euro}$) in the event that a generating unit has to be disconnected in order to reach a feasible terminal state. Such fee would reflect not only the shut-down cost of a generating unit but also the fact that the unexpected disconnection may disrupt the unit's planned operating schedule for the subsequent periods due to minimum down-time restrictions. Evidently, the level of this fee would depend both on the technical characteristics of every generating unit (*i.e.* capacity, flexibility *etc.*) as well as on its connection point to the network.

(vii) Given that through (3) and (4) the present formulation explicitly controls the severity arising from the realization of any contingency $c \in \mathcal{N}_c$ and every possible post-contingency corrective control behavior $b \in \mathcal{N}_b$, we allow for the relaxation of the post-contingency transmission capacity limits under the corrective control working behavior. In the event that such limits have been relaxed at the optimal solution, we model the consequences of such a decision as described in approximation (iv), *i.e.* we remove the overloaded branches from service prior to seeking for a feasible terminal state.

The effect of all such approximations on the findings of this paper, as well as the potential for reconsideration will be discussed in detail at the final parts of this paper.

III. Mathematical Formulation

In the present section we introduce the detailed form of the security management problem under consideration. We note that problem (7)-(41) can be cast as a Mixed-Integer Linear Programming Problem (MILP) by employing the linearization technique detailed in appendix A.

$$\min \left\{ \sum_{g \in N_g} c_g \cdot P_g^0 + \sum_{c \in N_c \setminus 1} \pi_c \cdot c_g^r \left(P_g^c - P_g^0 \right) \right.$$
$$\left. + \sum_{c \in N_c \setminus 1} \pi_c \cdot \sum_{b \in N_b} \pi_b \cdot s^c(b) \right\} \tag{7}$$

subject to,

for all nodes $n \in \mathcal{N}_n$:

$$\sum_{g \in \mathcal{G}_n} P_g^0 - \sum_{\ell \in \mathcal{N}_\ell} \beta_{n,\ell} \cdot f_\ell^0 = \sum_{d \in \mathcal{D}_n} P_d^0 \tag{8}$$

for all lines $\ell \in \mathcal{N}_\ell$

$$f_\ell^0 - \frac{1}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \theta_n^0 = 0 \tag{9}$$

$$f_\ell^0 \le f_\ell^{max} \tag{10}$$

$$- f_\ell^0 \le f_\ell^{max} \tag{11}$$

for all generators $g \in \mathcal{N}_g$

$$P_g^0 \le P_g^{max} \tag{12}$$

$$- P_g^0 \le -P_g^{min} \tag{13}$$

for all nodes $n \in \mathcal{N}_n$, all contingencies $c \in \mathcal{N}_c$ and corrective control working behavior:

$$\sum_{g \in \mathcal{G}_n} P_g^c - \sum_{\ell \in \mathcal{N}_\ell} \beta_{n,\ell} \cdot f_\ell^c(b) = \sum_{d \in \mathcal{D}_n} P_d^0 \tag{14}$$

for all nodes $n \in \mathcal{N}_n$, all contingencies $c \in \mathcal{N}_c$ and corrective control failing behavior:

$$\sum_{g \in \mathcal{G}_n} a_g^c \cdot P_g^0 - \sum_{\ell \in \mathcal{N}_\ell} \beta_{n,\ell} \cdot f_\ell^c(b) + \delta_n^c(b) = \sum_{d \in \mathcal{D}_n} P_d^0 \tag{15}$$

$$\delta_n^c(b) - \tau_c \cdot \sum_{g \in \mathcal{G}_n} \left(P_g^c - P_g^0 \right) = 0 \tag{16}$$

for all lines $\ell \in \mathcal{N}_\ell$, all contingencies $c \in \mathcal{N}_c$ and all corrective control behaviors $b \in N_b$:

$$f_\ell^c(b) - \frac{a_\ell^c}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \theta_n^c(b) = 0 \tag{17}$$

$$f_\ell^c(b) - a_\ell^c \cdot \lambda_\ell^c(b) \cdot M \le a_\ell^c \cdot f_\ell^{max} \tag{18}$$

$$- f_\ell^c(b) - a_\ell^c \cdot \lambda_\ell^c(b) \cdot M \le a_\ell^c \cdot f_\ell^{max} \tag{19}$$

$$f_\ell^c(b) - p_\ell^c(b) \cdot M \le 0 \tag{20}$$

$$- f_\ell^c(b) - (1 - p_\ell^c(b)) \cdot M \le 0 \tag{21}$$

$$\lambda_\ell^c(b) - \frac{f_\ell^c(b)}{f_\ell^{max} + \varepsilon} - (1 - p_\ell^c(b)) \cdot M \le 0 \tag{22}$$

$$\lambda_\ell^c(b) + \frac{f_\ell^c(b)}{f_\ell^{max} + \varepsilon} - p_\ell^c(b) \cdot M \le 0 \tag{23}$$

for all generators $g \in \mathcal{N}_g$ and all contingencies $c \in \mathcal{N}_c$

$$P_g^c \le a_g^c \cdot P_g^{max} \qquad (24)$$

$$-P_g^c \le -a_g^c \cdot P_g^{min} \qquad (25)$$

$$P_g^c - a_g^c \cdot P_g^0 \le a_g^c \cdot P_g^+ \qquad (26)$$

$$a_g^c \cdot P_g^0 - P_g^c \le a_g^c \cdot P_g^- \qquad (27)$$

for all nodes $n \in \mathcal{N}_n$, all contingencies $c \in \mathcal{N}_c$ and all corrective control behaviors $b \in N_b$:

$$\sum_{g \in \mathcal{G}_n} \hat{P}_g^c(b) - \sum_{\ell \in \mathcal{N}_\ell} \beta_{n,\ell} \cdot \hat{f}_\ell^c(b) - \sum_{d \in \mathcal{D}_n} \hat{P}_d^c(b) = 0 \qquad (28)$$

for all lines $\ell \in \mathcal{N}_\ell$, all contingencies $c \in \mathcal{N}_c$ and corrective control working behavior:

$$\hat{f}_\ell^c(b) - \frac{a_\ell^c \cdot (1 - \lambda_\ell^c(b))}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \hat{\theta}_n^c(b) = 0 \qquad (29)$$

$$\hat{f}_\ell^c(b) - a_\ell^c \cdot (1 - \lambda_\ell^c(b)) \cdot f_\ell^{max} \le 0 \qquad (30)$$

$$-\hat{f}_\ell^c(b) - a_\ell^c \cdot (1 - \lambda_\ell^c(b)) \cdot f_\ell^{max} \le 0 \qquad (31)$$

for all lines $\ell \in \mathcal{N}_\ell$, all contingencies $c \in \mathcal{N}_c$ and corrective control failing behavior:

$$\hat{f}_\ell^c(b) - \frac{a_\ell^c \cdot (1 - \tau_c \cdot \lambda_\ell^c(b))}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \hat{\theta}_n^c(b) = 0$$
$$\qquad (32)$$

$$\hat{f}_\ell^c(b) - a_\ell^c \cdot (1 - \tau_c \cdot \lambda_\ell^c(b)) \cdot f_\ell^{max} \le 0 \qquad (33)$$

$$-\hat{f}_\ell^c(b) - a_\ell^c \cdot (1 - \tau_c \cdot \lambda_\ell^c(b)) \cdot f_\ell^{max} \le 0 \qquad (34)$$

for all demands $d \in \mathcal{N}_n$, all contingencies $c \in \mathcal{N}_c$ and corrective control behaviors $b \in N_b$:

$$\hat{P}_d^c(b) \le P_d^0 \qquad (35)$$

for all generators $g \in \mathcal{N}_g$, all contingencies $c \in \mathcal{N}_c$ and corrective control working behavior:

$$\hat{P}_g^c(b) - \left(1 - y_g^c(b)\right) \cdot P_g^c \le 0 \qquad (36)$$

$$-\hat{P}_g^c(b) + \left(1 - y_g^c(b)\right) \cdot \left(P_g^c - a_g^c \cdot \Delta P_g^e\right) \le 0 \qquad (37)$$

for all generators $g \in \mathcal{N}_g$, all contingencies $c \in \mathcal{N}_c$ and corrective control failing behavior:

$$\hat{P}_g^c(b) - a_g^c \cdot \left(1 - y_g^c(b)\right) \cdot P_g^0 \le 0 \qquad (38)$$

$$-\hat{P}_g^c(b) + a_g^c \cdot \left(1 - y_g^c(b)\right) \cdot \left(P_g^0 - \Delta P_g^e\right) \le 0 \qquad (39)$$

for all generators $g \in \mathcal{N}_g$, all contingencies $c \in \mathcal{N}_c$ and corrective control behaviors $b \in \mathcal{N}_b$:

$$-\hat{P}_g^c(b) + a_g^c \cdot \left(1 - y_g^c(b)\right) \cdot P_g^{min} \le 0 \qquad (40)$$

for all contingencies $c \in \mathcal{N}_c$ and corrective control behaviors $b \in \mathcal{N}_b$:

$$-s^c(b) + \sum_{d \in \mathcal{N}_d} v_d \cdot (P_d^0 - \hat{P}_d^c(b)) + \sum_{g \in \mathcal{N}_g} w_g \cdot y_g^c(b) \le 0$$
$$\qquad (41)$$

$$s^c(b) - \gamma^c(b) \cdot M \le s_{max} \qquad (42)$$

$$\sum_{c \in \mathcal{N}_c} \pi_c \cdot \sum_{b \in \mathcal{N}_b} \pi_b \cdot \gamma^c(b) \le \epsilon \qquad (43)$$

The first term in (7) expresses the cost of the preventive generation schedule while the second denotes the expected cost of the corrective re-dispatch. The third term is the expectation of the severity function. We underline that the form of the first two terms of (7) depends on the applicable regulatory framework. Without loss in generality, through function (7) we consider the case wherein a TSO seeks to minimize the expected net generation cost under any credible event. The extension of this work to alternative regulatory arrangements, *e.g.* in the case wherein the TSO is accountable for the cost of changes with respect to the outcome of an already settled market clearing, remains straightforward (see appendix B).

The pre-contingency nodal power balance is enforced via equality (8). Expressions (9) to (11) correspond to the DC power flow approximation and line capacity limits in the pre-contingency state respectively. Moreover, the feasible operating region of the generating units in the pre-contingency state is expressed by (12)-(13).

The post-contingency nodal power balance is expressed through (14) and (15). The former holds for the case that there is no failure in the corrective control, hence the equality is strictly enforced. We underline that, in case the contingency relates to the outage of a generating unit, the ineffectiveness of the corrective re-dispatch would result in an energy mismatch. To account for this effect in (15), we introduce a free slack variable ($\delta_n^c(b)$) per node. Equality (16) defines the value of such slack variable with the use of auxiliary binary parameter τ_c, which would only take a value of 1 for a generator outage.

The DC power flow approximation in the post-contingency states is expressed by (17). Binary variable $\lambda_\ell^c(b)$ is used in (18) and (19) to allow for the relaxation of the line capacity limits. To achieve that this variable would only take a value of one when the capacity limits are exceeded, logical constraints (20) through (23) are used[7]. More specifically, (20) - (21) enforce that the value of binary variable $p_\ell^c(b)$ would be equal to one if the flow is positive (zero if the flow is negative). In the former case, (22) imposes that binary variable $\lambda_\ell^c(b)$ can only be equal to one if the flow is (at least infinitesimally) greater than the corresponding limit, while (23) is inactive. Conversely, in the case that the sign of $f_\ell^c(b)$ is negative, (23) takes force to ensure that a non-zero value of binary variable $\lambda_\ell^c(b)$ indicates an overload while (22) is inactive.

[7]Symbol ε denotes an infinitesimally small constant.

The feasible operating region of the generating units in the post- contingency states is expressed via (24)-(27). Coupling constraints (26) and (27) are used to consider ramping restrictions.

In order to quantify the severity of the system state, we seek for a feasible power flow solution following the realization of the effects of corrective control behavior. More specifically, expression (28) re-establishes the nodal power balance constraint. Furthermore, (29)-(34) impose that overloaded network branches would be disconnected[8]. We note that the products of binary and continuous variables appearing in (29)-(34) can be linearized according to the methodology presented in appendix A.

The set of admissible emergency control actions is modeled via (35)-(40). Inequality (35) allows the use of load shedding as a measure of last resort. Constraints (36) through (39) impose that the generating units should either only ramp-down within a limited range (following the shedding of load) or be disconnected from the network. More specifically, (36) and (37) apply in the case wherein corrective control has been effective. In such a case, the emergency ramp-down limit would apply with respect to the post-contingency dispatch of any generating unit. Alternatively, in the case that corrective control has proven ineffectual, the limit is applicable with respect to any unit's preventive dispatch, as in (38) and (39). In both cases, if a generating unit has to ramp down beyond the admissible limit, binary variable $y_g^c(b)$ would take a value of one to denote the disconnection of this unit[9]. Likewise, (40) expresses the minimum stable generation restriction which remains valid.

Taking these measures used to reach a terminal state into account, the severity of the system state is expressed as in (41). The first term of (41) gathers the value of the load that cannot be served. As already mentioned, through the second term, we consider a fixed cost in the case that a generating unit has to be disconnected from the network. We recall that, parameter w_g essentially denotes the importance of ensuring the continuity in the connection of unit g to the network. Such parameter would be unit specific and depend not only on the capacity of the unit but also on its location in the network and its flexibility characteristics. Finally, inequalities (42) and (43) impose the chance constraint on the severity level through the use of auxiliary binary variable $\gamma^c(b)$.

IV. Single-Area Case Study

In the interest of establishing the novel features of the proposed approach we begin by discussing a set of demon-

[8]We should clarify that auxiliary binary parameter τ_c is used in (32)-(34) to maintain all network branches in service in the case that corrective control failed following a generator outage. This is due to the fact that, as explained earlier, in such a case the nodal power balance in the post-contingency state (15) can only be achieved by introducing a set of slack variables.

[9]The linearization of products of binary and continuous variables in (36) and (37) is presented in Appendix A as well.
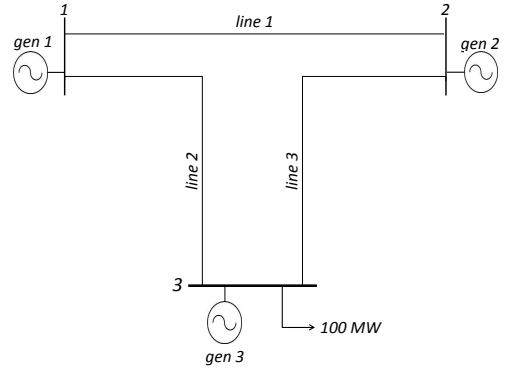

Fig. 2. Three-node, three-generator system

TABLE I
Generating Units Specifications

g	c_g ($€/MWh$)	c_g^r	P_g^{min} (MW)	P_g^{max}	MTTF (h)	w_g ($€$)
1	20	5	10	100	500	4000
2	40	8	10	100	500	4000
3	30	7	10	50	250	4000

strative case studies based on the 3-bus network of figure 2. Table I summarizes the parameters of the 3 generating units[10]. All network branches are assumed to have a maximum capacity of 55 MW, equal admittance and a mean time to failure of 10000 h, as in [15]. The demand at node 3 is assumed to be equal to 100 MW for a period of 1 hour, while the value of lost load is set at €300/MWh.

We underline that for the purposes of these demonstrative cases studies and without loss in generality, both the value of lost load (v_d) as well as the generating units' disconnection severity coefficients (w_g) have been arbitrarily set. In the interest of signifying the value of maintaining service to the network users, the former was set an order of magnitude greater than the per unit generation costs in the test system. Recalling that the latter should reflect costs incurred at the period of disconnection as well as the criticality of disrupting the availability of supply for the forthcoming periods, a considerably large value was selected. The critical role of such parameters on the performance of the proposed approach, as well as the necessity of establishing credible reference values, will be discussed in detail at the concluding parts of this paper.

The set of credible failures considered in this example involves the failure of any single component. The probabilities of all credible contingencies, including the pseudo-contingency of no failure, have been calculated according to [16] and are listed in table II. Following the occurrence of any contigency, we assume that the probability of realization of the corrective control working behavior is

[10]For the sake of simplicity, ramping restrictions have been omitted in this example.

TABLE II
Contingency Set

c	Event	π_c
1	No Outage	0.99193
2	Line 1 Outage	$0.9 \cdot 10^{-4}$
3	Line 2 Outage	$0.9 \cdot 10^{-4}$
4	Line 3 Outage	$0.9 \cdot 10^{-4}$
5	Gen. 1 Outage	$1.9 \cdot 10^{-3}$
6	Gen. 2 Outage	$1.9 \cdot 10^{-3}$
7	Gen. 3 Outage	$4 \cdot 10^{-3}$

TABLE III
Case A: Preventive Dispatch (MW)

g	1	2	3
	77.5	10	12.5

0.8.

A. Case A: The 'hidden' severity levels of the N-1 approach

In order to establish a benchmark for comparison, we begin by presenting the sequence of preventive and corrective actions under the N-1 approach. This sequence has been identified by simplifying the formulation presented in section III in the following ways:

- The third term of (7) has been omitted.
- A sufficiently large admissible severity threshold, making constraints (42)-(43) ineffectual, has been selected.
- All constraints referring to the corrective control working behavior have been strictly enforced, while all constraints referring to the corrective control failing behavior can be relaxed.

Owing to these simplifications, decision making in case A follows the assumption that corrective control is fully reliable. Nevertheless, the effects of the possible failure of corrective control, as well as the resulting severity levels are computed as by-products of the optimization process.

The preventive generation schedule as well as the corrective re-dispatch under any credible contingency are

TABLE IV
Case A: Corrective Re-dispatch (MW)

$c \setminus g$	1	2	3
2	55	10	35
3	45	10	45
4	45	10	45
5	x	50	50
6	82.5	x	17.5
7	65	35	x

TABLE V
Case A: Power Flows under Corrective Control Failure (MW)

$c \setminus \ell$	1	2	3
2	x	**77.5**	10
3	**77.5**	x	**87.5**
4	-10	**87.5**	x

TABLE VI
Case A: Severity Levels

c	2	3	4	5	6	7
$s^c(b)$ (€)	27250	34250	34250	23250	3000	3750
$s^c(b)$ (%)	64.88	81.55	81.55	55.36	7.14	8.92
$\pi_c \cdot \pi_b \cdot 10^{-4}$	0.18	0.18	0.18	3.8	3.8	8

presented in tables III and IV respectively. Evidently, under the corrective control working behavior the system expected severity is zero since there exists a combination of preventive and corrective actions to serve the demand under any contingency. Nevertheless, it is also evident that the sequence of actions listed in tables III and IV is not resilient against the possibility that the corrective re-dispatch may not materialize.

In fact, for generating unit outages the occurrence of an energy deficit would be inevitable. Acknowledging that all line outages ($c = 2, \ldots, 4$) would require re-dispatch actions (by inspecting table III and rows 1-3 of table IV) we can identify that network capacity ratings would be exceeded in case corrective control failed to take effect. Indeed, this is confirmed in table V, wherein the line flow patterns under the corrective control failing behavior are presented for these contingencies.

Table VI presents the potential severity levels (first row) along with the corresponding probabilities of realization (third row). As an example, figure 3 illustrates the potential effect of corrective control failure following contingency 3. In such a case, the failure of corrective control would result in overloading both network branches that were not affected by the initiating contingency. Acknowledging that these overloaded branches would be subsequently taken out of service, all 3 network nodes would eventually be isolated. Consequently, generating units 1 and 2 would have to be disconnected due to minimum stable generation restrictions. Moreover, given that controllability of generating unit 3 is assumed to be lost, the maximum available generation to serve the demand is $12.5MW$, *i.e.* the pre-contingency output of unit 3. As a result $87.5MW$ of demand would have to be shed for a period of 1 hour.

Noting that the maximum possible severity level in the present example is equal to €42000 (in the case that all units are disconnected and none of the demand is served) the second row of table VI presents a relative
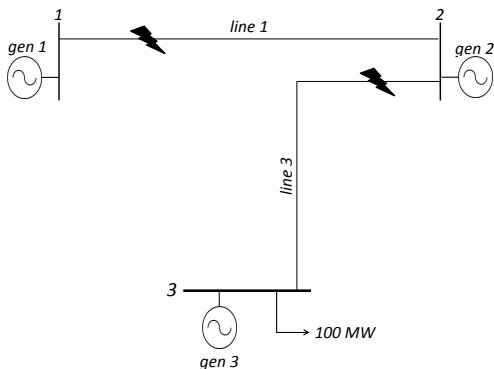
Fig. 3. Failure of Corrective Control under Outage of Line 2

TABLE VII
Case B: Preventive Dispatch (MW)

g	1	2	3
	45	10	45

TABLE VIII
Case B: Corrective Re-dispatch (MW)

$c \setminus g$	1	2	3
2	55	10	35
3	45	10	45
4	45	10	45
5	x	50	50
6	82.5	x	17.5
7	65	35	x

TABLE IX
Case B: Power Flows under Corrective Control Failure (MW)

$c \setminus \ell$	1	2	3
2	x	45	10
3	45	x	55
4	-10	55	x

comparison. We should conclude by stating that the cost of the preventive generation schedule in this case is €2325 while the expected cost of the corrective redispatch is €0.55. Relative to the latter figure, the expected severity level of €14.7 appears non-negligible.

B. Case B: Acknowledging the Severity of Corrective Control Potential Failure

The second case study serves to demonstrate the effect of considering the potential failure of corrective control via controlling the system severity levels. To that end, we now consider the complete formulation presented in section III. For the sake of consistency, we begin by maintaining from case A the constraint that the line capacity limits should not be relaxed under the corrective control working behavior. The potential relaxation of these capacity limits will be investigated at a subsequent part of this case study.

The admissible severity threshold is set at 33% (1/3) of the largest possible severity value, *i.e.* $s_{max} = 14000$ €. We begin by considering this threshold as a hard constraint by setting the upper bound on the severity violation probability to zero. The effect of chance constraint (42)-(43) on the severity threshold violation will also be demonstrated at a following part of this case study.

Tables VII and VIII present the preventive dispatch and corrective re-dispatch. In comparison to case A (tables III and IV) we can identify that the corrective re-dispatch remains unaltered. This was anticipated given the fact that in case A, the severity levels under the corrective control working behavior were equal to zero for all contingencies. Likewise as expected, the difference between cases A and B lies in the preventive schedule. The preventive schedule implemented in case B comes at an increased cost since generating unit 3 is now displacing cheaper unit 1.

Such cost increase comes at the benefit of ensuring that the severity level is always below the desirable threshold, even under the potential failure of corrective control. In order to achieve this requirement, the selected preventive

dispatch is feasible under all line outages, table IX. Given this fact, it is noteworthy that a corrective re-dispatch has also been selected. This is due to the fact that in case the corrective control does not fail to have an effect, the re-dispatch would generate a cost reduction. In this sense, the secure preventive dispatch serves as a fall-back for the case that corrective control is ineffectual. As a result, the severity under corrective control failure for all line outages has been eliminated, table X. Nevertheless, the energy mismatches arising from generation outages when corrective control is ineffectual can only be counteracted by means of emergency load shedding. As such, the severity levels for all generating unit outages remain non-zero. On average, these levels are lower than case A though.

Finally, in table XI we compare the preventive and expected corrective costs, as well as the expected severity levels between cases A and B. As anticipated, the preventive cost of case B is greater than that of case A. It should be noted that this cost increase is asymmetrical to the reduction of the expected severity level. This asymmetry serves to demonstrate the conceptual difference between the monetary and non-monetary costs of power system

TABLE X
Case B: Severity Levels

c	2	3	4	5	6	7
$s^c(b)$ (€)	0	0	0	13500	3000	13500
$s^c(b)$ (%)	0	0	0	32.14	7.14	32.14
$\pi_c \cdot \pi_b \cdot 10^{-4}$	0.18	0.18	0.18	3.8	3.8	8

TABLE XI
COMPARISON OF COST COMPONENTS (€)

	Preventive Cost	$\mathbb{E}\{$Corrective Cost$\}$	$\mathbb{E}\{$Severity$\}$
Case A	2325	0.55	14.7
Case B	2650	0.03	9.3

TABLE XII
COMPARISON OF ALTERNATIVE CHANCE LEVELS

	P_g^0	(MW)	
$\epsilon \setminus g$	1	2	3
1	45	10	45
2	77.5	10	12.5

TABLE XIII
CASE B: PREVENTIVE DISPATCH WITH POTENTIAL CAPACITY LIMIT RELAXATION (MW)

g	1	2	3
	45	10	45

TABLE XIV
CASE B: CORRECTIVE RE-DISPATCH WITH POTENTIAL CAPACITY LIMIT RELAXATION (MW)

$c \setminus g$	1	2	3
2	55	10	35
3	45	10	45
4	45	10	45
5	x	50	50
6	82.5	x	17.5
7	65	35	x

security. We recall that in the present case, the admissible severity threshold was considered as a hard constraint. Owing to the fact that the severity target was thus prioritized, the system operational costs became a less critical factor in the decision making process and were consequently increased.

On the Utility of the Probabilistic Chance Constraint: As cases A and B have exemplified, security management involves trade-offs between monetary and societal costs. We recall that in case A, a smaller operational cost was achieved at the expense of neglecting the (low-probability) likelihood of very high severity levels. Arbitrating between high consequence, lower probability situations and the corresponding security costs has thus far been implicit under the N-1 criterion. The present case study serves to demonstrate that the proposal of this paper allows for an explicit arbitrage between these factors.

To that end, we reconsider the example of figure 2 under two different upper bounds on the severity violation probability. A value of $\epsilon_1 = 10^{-5}$, *i.e.* lower than the probability of realization of the high severity levels of case A, and a value of $\epsilon_2 = 10^{-2}$. As table XII demonstrates, the solution to the former case corresponds to the solution of case B. This is due to the fact that the probability of realization of the combination of contingencies and corrective control behaviors is greater than the upper bound on the severity violation probability. As such, the potential severity levels for these system states are to be controlled. Likewise, the solution to the case where $\epsilon_2 = 10^{-2}$ is the solution of case A since the severity threshold can be violated with a probability greater than the probability of realization of these states. In this manner, the present formulation allows for selecting the set of events against which the system should be protected by quantifying the relative costs and benefits.

On Relaxing the Line Capacity Limits: As a final point for consideration in this set of case studies, we return to the fact that the proposal of this paper allows for a relaxation of the post-contingency line capacity limits. The sole criterion for allowing or prohibiting such a decision remains the resulting societal cost. This property has been demonstrated between cases A[11] and B. In the former, line capacity limits under the corrective control failing behavior have been relaxed at the optimal solution. This was a result of the fact that the corresponding severity levels were admissible according to the respective threshold and violation probability upper bound. As in the latter this was not the case, line capacity limits in the corrective control failing behavior were not relaxed at the optimal solution.

In order to exemplify the efficiency of this approach with clarity, we conclude by presenting the solution to case B when the line capacity limits are allowed to relax even under the corrective control working behavior, tables XIII and XIV. As these tables demonstrate, this solution is identical to the initial solution of case B, since the relaxation these limits at the optimal solution would result in non-admissible severity levels. The fact that the identification of the conditions under which these limits can be relaxed is efficient, justifies the consideration of this additional degree of freedom to the decision maker.

V. Multi-Area Case Study

In the second set of case studies, we focus on the stakes of implementing the proposed approach across several areas of an interconnected power system. The scope of these case studies is to identify the combined effects of different security management practices on all end-users, located in different control areas of the system.

To that end, we consider the six-node, two area system presented in figure 4. Area A comprises nodes (1-3) while nodes (4-6) form area B. The specifications of the 5 generating units are presented in tables XV and XVI. Table XVII lists the maximum capacity of the transmission lines,

---

[11]We recall that this case is identical to the full formulation when the maximum admissible severity level has a considerably large value.
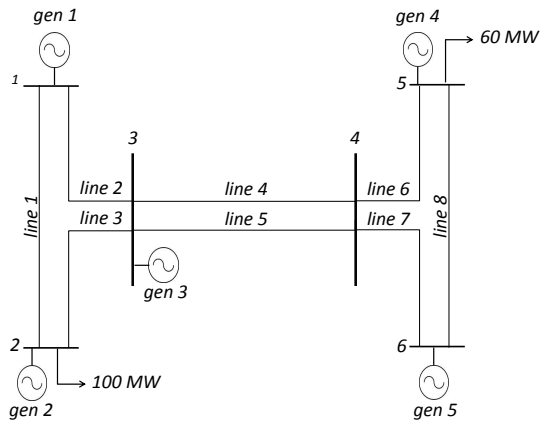
Fig. 4. Six-node, two area system

TABLE XV
GENERATING UNITS TECHNICAL CHARACTERISTICS

g	P_g^{min}	P_g^{max}	P_g^-	P_g^+	ΔP_g^e	MTTF
			(MW)			h)
1	10	100	40	40	5	500
2	10	100	20	40	5	500
3	10	50	40	40	5	250
4	100	10	40	40	5	250
5	40	5	20	20	5	250

TABLE XVI
GENERATING UNITS COST DATA

g	c_g (€/MWh)	c_g^r (€/MWh)	w_g (€)
1	20	5	2500
2	40	8	2500
3	30	7	2500
4	65	10	4000
5	50	8	4000

which are again assumed to have an equal admittance and a mean time to failure of 10000 hours. Finally, table XVIII shows the allocation of the severity coefficients across the two areas of the system. As this table indicates, area A is assumed to be of lower per unit severity (both in terms of shedding load and disconnecting generating units) with respect to area B.

TABLE XVII
TRANSMISSION CAPACITY (MW)

ℓ	f_ℓ^{max}
1	65
$2-7$	55
8	65

TABLE XVIII
SEVERITY COEFFICIENTS

Area	v_d (€/MWh)	w_g (€)
A	150 $\{d=1\}$	2500 $\{g \in [1,3]\}$
B	300 $\{d=2\}$	4000 $\{g \in [4,5]\}$

TABLE XIX
SYSTEM-WIDE SECURITY MANAGEMENT SEVERITY LEVELS(€)

N-1 Approach			
Event	Total	Area A	Area B
Line 1/Control Fail.	19750	13750 (69.6%)	6000 (30.4%)
Line 2/Control Fail.	16750	16750	0
Line 3/Control Fail.	19750	13750 (69.6%)	6000 (30.4%)
Gen 1/Control Fail.	14250	14250	0
Gen 2/Control Fail.	3750	3750	0
Gen 3/Control Fail.	1500	1500	0
Gen 4/Control Fail	750	750	0
Severity Controlled Approach			
Event	Total	Area A	Area B
Gen 1/Control Fail.	8250	8250	0
Gen 2/Control Fail.	6750	6750	0
Gen 3/Control Fail.	6750	6750	0
Gen 4/Control Fail.	1500	1500	0
Gen 5/Control Fail.	750	750	0

A. System-wide Security Management

In order to set a basis for comparison, we begin by considering that both areas are under the control of a common operator. In this context, we compare the effect of the proposed severity controlled approach against the N-1 across the two system areas. The set of credible contingencies includes the single failure of any system component. As in the previous section, we assume that the probability of corrective control failure is equal to 0.2. The admissible severity threshold is set at 25% of the maximum severity across both areas (*i.e.* $s_{max} = 12125$ €). Finally, we consider this threshold as a hard constraint by setting the respective violation probability allowance to zero.

Table XIX analytically compares the potential severity levels between the N-1 and the proposed severity controlled approach[12]. As anticipated, the potential severity levels are greater under the N-1 approach. The allocation of the potential severity levels between the two areas is also of interest. Under the severity controlled approach, impacts to the end-users are always restricted within the low per unit severity area (area A). Nevertheless, this is not the case for the N-1 approach. We recall that under the N-1 approach the potential failure of corrective control is completely neglected. As such, there exist possible combinations of preventive control actions and corrective

[12]For the sake of the presentation simplicity, only events with non-zero severity values are henceforth listed.

TABLE XX
System-wide Optimal Power Flow (*MW*)

P_1^0	P_2^0	P_3^0	P_4^0	P_5^0
100	10	35	10	5

TABLE XXI
Preventive Dispatch Comparison (*MW*)

Control	P_1^0	P_2^0	P_3^0	P_4^0	P_5^0
System	55	45	45	10	5
Area A	60	70	45	10	5

TABLE XXII
Severity Levels (€)

Severity Controlled Approach in Area A			
Event	Total (€)	Area A	Area B
Gen 1/Control Fail.	18000	0	18000
Gen 2/Control Fail.	19500	1500	18000
Gen 3/Control Fail.	4500	0	4500
Line 1/Control Fail.	20500	2500	18000

control behaviors under which service disruption within the high per unit severity area is inevitable.

B. Area-wide Security Management

In the present subsection we consider the case wherein the two interconnected areas A and B are under the responsibility of different operators. Moreover, we consider that the operator of area A follows the proposed severity controlled approach while the operator of area B follows the N-1 practice. In the former occasion, the admissible severity threshold is set at 25% of the maximum severity within area A and the violation probability allowance is once again equal to zero.

In order to evaluate the minimum system wide severity levels we adopt the following process:

- We consider two separate security management sub-problems concerning areas A and B. In both cases, the respective operator can only apply preventive and corrective actions (and face the associated costs) within its area of interest. Moreover, the set of credible contingencies involves any single failure within the area under the responsibility of the respective operator as well as the failure of any single area interconnector.
- Given that the solution of subsection 2.1 only covers single failures, we assume that the occurrence of a contingency outside of the respective operator's control area is not a credible event. As such, we set the operating point of the generating units in the area outside the control of the respective operator according to the solution of an OPF concerning the two-area interconnected system, table XX.
- Within the security management subproblem of operator A (adopting the severity controlled approach) we take into account the fact that it's jurisdiction does not extend outside area A. On this basis, we prevent the relaxation of any constraints within area B under any possible system state.
- Within the security management subproblem of operator B (adopting the N-1 approach) we take into account the fact that the neglected potential failure of corrective control may cause constraint violations within area A as well.
- Following the solution of subproblems concerning areas A and B we merge all identified corrective and preventive decisions and seek to minimize the net severity level across both areas under any credible state by means of emergency control actions.

1) Severity Controlled Approach within Area A: The scope of operator A is to optimize the value of (7) while maintaining the potential severity levels within area A below €5625 (*i.e.* 25% of the maximum possible severity within area A). By inspecting rows 8-10 of table XIX, which concern contingencies within area A, we can identify that the system wide security management strategy fails to achieve this target. We underline that all concerned instances are under the failure of corrective control. As such, operator A should seek for an alternative preventive dispatch to restrict the impact of these events. As demonstrated in table XXI, the preventive actions selected by operator A differ with respect to the case where the severity controlled approach is implemented across both system areas.

Evidently, the change in the preventive dispatch also gives rise to a change in the corrective re-dispatch. Table XXII demonstrates the optimal severity levels from the perspective of area A operator. We note that rows 1-3 of XXII correspond to rows 8-10 of table XIX. All these events concern the failure of corrective control following the occurrence of a generating unit outage. The corresponding non-zero severity levels of these events denote the necessity of emergency load shedding across the system. In the present case, transmission network constraints are not restrictive to impose whether load should be shed within area A or area B to alleviate the mismatch. Under these conditions, from the perspective of operator A, the acceptable solution would be to transfer the impact of the energy mismatch to area B, by prioritizing the disruption of the demand connected at node 5.

In order to exemplify the values listed in the last row of XXII, we present in figure 5 the network configuration following the outage of line 1 and the failure of corrective control. We recall, that in such an occasion all generating units would remain at the operating points listed in the second row of table XXI. Consequently, the 60 MW of injection at node 1 would result in the overload of line 2, which has a maximum capacity limit of 55 MW. The loss of this line would result in an deficit of 60 MW. Considering, once again that such a deficit can be alleviated by shedding
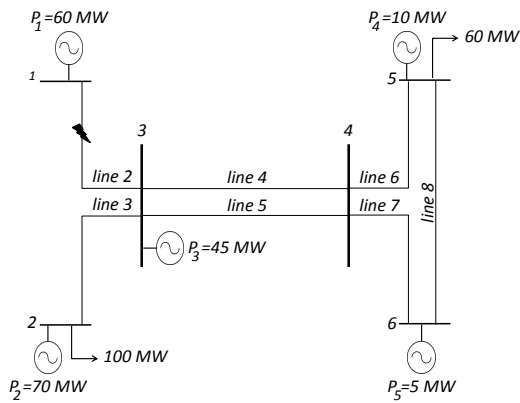
Fig. 5. Failure of Corrective Control under Outage of Line 1

TABLE XXIII
Minimum System-wide Severity Levels (€)

Event	Total	Area A	Area B
Line 1/Control Fail.	11500	11500	0
Gen 1/Control Fail.	9000	9000	0
Gen 2/Control Fail.	10500	10500	0
Gen 3/Control Fail.	2250	2250	0
Gen 4/Control Fail.	1500	1500	0
Gen 5/Control Fail.	750	750	0

the load at node 5 operator A deems this event acceptable. In the event that the load at node 5 is shed, the sole impact in area A would be the disconnection of unit 1 at a severity of €2500.

2) N-1 Approach within Area B: For the sake of completeness, we briefly discuss the adoption of the N-1 approach within area B. By inspecting table XV we can identify that the minimum stable restrictions of generating units 4 and 5 prohibit any reconsideration of the operating points listed in table XX. Considering the network topology (figure 4) as well as the line capacity limitations (table XVII), such operating point is feasible under any single line outage within area B, as well as the outage of any single interconnector. As a result, the N-1 approach in area B would only involve corrective actions in the case any one of the two generating units trips.

3) The Combined Effect of the Different Security Management Practices: We conclude by assessing the combined effect of implementing different security management approaches in the two areas of the interconnected system of figure 4. For this purpose, we re-compute the system-wide optimal severity levels in the case where the preventive and corrective strategies for areas A and B have been identified according to the severity controlled approach and the N-1 approach respectively.

As table XXIII demonstrates, in order to minimize the system-wide severity levels the impact of any event should be once again restricted within area A. We highlight the fact that the potential severity levels in area A are

TABLE XXIV
Area A Security Management Costs (€)

Control	Preventive Cost	$\mathbb{E}$\{Corrective Cost\}	$\mathbb{E}$\{Severity\}
System	4250.5	-1.58	12.44
Area A	4450	-0.318	10.88

considerably greater with respect to the values listed in table XIX. Evidently, this is due to the fact that the actual criticalities of the end-users located at area B where completely neglected by area A operator under the severity controlled approach.

Table XXIV presents a comparison of the cost breakdown in area A between the case wherein the severity controlled approach was adopted in both areas of the interconnected system and the case where the severity controlled approach was adopted only in area A. Recalling that the need to control the severity under corrective control failure drives the operator towards more expensive preventive control strategies justifies the observed increased in the preventive cost. In the system-wide case a larger severity threshold was available to the operator. We observe once again from table XIX that such large threshold allowed the severity in area A to reach values above 25% of the maximum possible area A severity. As in the case where severity control is only implemented in area A the 25% of the maximum area severity must be enforced, a more conservative, hence more expensive, preventive dispatch has been selected.

In both cases, the negative terms related to the expected corrective control costs highlight the push toward the more conservative preventive control strategies. These negative terms denote that the preventive schedules are so conservative that if a failure indeed triggers the operation of corrective control system costs can be reduced. We should finally clarify the origin in the observed reduction in the expected severity value. Even though the severity levels listed in table XXIII exceed those of table XIX, the considerable reduction in case that corrective control has failed following the outage of unit 3, along with the relatively large probability of realization of this event, lead to a reduced expected value.

Table XXV introduces a similar comparison for Area B. As already noted, the preventive dispatch remains unaltered in the case that area B follows the N-1 approach and the case where the severity controlled approach is implemented in the two system areas. Moreover, in both cases the potential severity levels would be equal to zero since the impact of any event would be directed toward the lower (per unit) severity area A. The increase in the expected corrective costs in the system-wide severity controlled case arises from the fact that generating units in area B are re-dispatched to counteract contingencies in area A.

TABLE XXV
Area B Security Management Costs (€)

Control	Preventive Cost	$\mathbb{E}\{$Corrective Cost$\}$	$\mathbb{E}\{$Severity$\}$
System	900	1.165	0
Area B	900	0.47	0

VI. Concluding Remarks

The N-1 practice has been pivotal to the secure operation of electrical power systems. On the core of this approach, lies a rigid attitude with regard to the uncertainties in power system operation. Events that are considered sufficiently likely (*i.e.* the outage of any single system component) are to be treated as threats to the system security whereas every other event is to be neglected. The vast experience from the operation of power systems to date has exemplified the resilience of this approach in the case the degree of uncertainty is relatively minor. Nevertheless, even under such case, the rare examples where this approach failed to protect the system have resulted in severe consequences to its end-users. This is due to the fact that the N-1 approach inherently disregards the difference in the risk levels between the different possible system operating points [17].

Nowadays, the growth of uncertainties is a well-acknowledged fact amongst the members of the power system community. To cater for this fact under the N-1 framework in an efficient manner, more and more corrective control measures have to be adopted. The increasing adoption of such measures may not fully warrant the security of modern power systems though. Understanding the behavior of corrective control and, most importantly, characterizing the uncertainties induced by its operation appear as preconditions to this task. In a different case, the use of corrective control measures would introduce hidden threats of potentially high consequences to the system security.

Considering these facts, in the present paper we investigated the utility of an alternative probabilistic security management approach. This approach departs from the N-1 practice in the following key aspects: i) the probability of realization of any credible system state is explicitly taken into account, ii) corrective control outcome is considered as an additional source of uncertainty in the system operation, iii) the potential consequences resulting from any combination of contingencies and corrective control outcome, both in terms of operational costs to the TSO and in terms of service end-users' interruption costs, serve as a criterion for the treatment of possible events as threats to be counteracted and iv) the possibility of inducing severe consequences to the end-users is explicitly controlled, by means of a probabilistic chance constraint.

We would like to stress that the proposed probabilistic framework is a *proper* generalisation of various determin-istic (preventive/corrective) SCOPF formulations used for security management in practice, in the sense that one can obtain these latter by setting $s_{\max}$ and ϵ to zero, by leaving out the expected cost of service interruption from the objective function, and by assuming particular choices of the corrective control behaviors. We also remark that, while this framework is designed as a tool for *designing* optimal combined preventive and corrective control strategies for real-time operation, it may as well be used as a tool for *evaluating* any other (partially or completely specified) alternative control strategy by translating it in the form of additional (hard, or possibly soft) constraints and incorporating these latter into the RTP formulation. These two characteristics enable, in particular, a fair comparison of the current deterministic security management criteria with the proposed probabilistic one, which is a necessary condition for gaining acceptance and enabling the migration in real-world practice.

Section III furthermore provides a detailed mathematical formulation of the proposed framework, under the DC approximation and some additional simplifying assumptions, yielding a MILP problem which can be efficiently solved with available tools, even for large-scale systems.

A. Main Findings

Albeit remaining at the *proof-of-concept* level, the initial findings of this work (demonstrated by example in sections IV and V) clearly establish the interest of pursuing this research direction.

The single-area case studies analyzed in section IV have, first and foremost, unveiled the limitations in the scope of the N-1 approach. In contrast, these case studies have demonstrated the greater potential of a probabilistic, severity controlled approach. By means of this analysis, we have established that the proposed approach is in principle efficient in arbitrating between the operational costs of security provision and the potential consequences of service interruption to the system end-users. Moreover, we have shown the fitness of achieving a probabilistic guarantee with respect to mitigating high consequence threats of low likelihood. Not to be neglected, the outcome of these case studies accords to the inevitable truth: achieving an enhanced security level comes at (possibly, dis-proportionally) greater monetary costs. It thus appears of critical importance to consider both factors in order to develop an efficient security management strategy.

The multi-area case studies of section V considered the effect of adopting two different security management practices within two sub-areas of an interconnected system. The findings of these case studies serve to raise the need for conformity in the practices adopted by TSOs within an interconnected system. We have demonstrated that without such conformity, a single TSO may fail to achieve the severity related targets within his own area of interest even in the case wherein his individual policy appears

effective in doing so. Given that the technical interconnection remains a physical reality, a 'myopic' perspective within a sub-area of the system may well be counter-productive. It follows that the efficient implementation of such a framework calls for additional information exchange amongst the TSOs in an interconnected system. As this case study exemplified, in order to make sound decisions, any single TSO must be accurately informed on the factors driving emergency control (*i.e.* range of controllability and criticalities of service disruption) in the system areas outside its jurisdiction.

B. Open Issues

The present work serves to establish the interest in migrating from the N-1 practice toward a probabilistic security management approach. We thus conclude by discussing a series of issues that remain open in the direction of realizing such a transition.

1) Characterizing the Behavior of Corrective Control: The unpredictability in the behavior of corrective control was adopted as a starting point for this work. Given the role of corrective control, even in today's power system security management, characterizing the behavior of this resource with high accuracy would be of critical importance. In the context of the proposal of this paper, further research would be required to identify an exhaustive set including all the possible failing behaviors of corrective control. Evidently, associating a credible probability value to any such failing behavior is also essential.

In addition to developing such a set, special care is required in order to accurately model the operation of emergency control. The scope for this activity would be to reflect all the dynamic phenomena occurring in subsequence to the realization of any possible corrective control failing behavior. We underline that achieving a high degree of accuracy while preserving the computational tractability of the decision making problem is a non-trivial task. With the intention of concentrating on the fundamental principles of the proposed security management practice in this work, less emphasis was placed thus far on the former. Given the criticality of this point on the proposed decision making framework, in the next stage of this research we will seek to identify an optimal trade-off between computational tractability and modeling accuracy.

2) Quantifying the Societal Cost of Service Interruptions: Evaluating the utility received by the electricity consumers has been an active field of research within the social sciences community (see, *e.g.* [18], [19]). Needless to say, this field lies well outside the scope of any engineering study. Be that as it may, we take this opportunity to highlight the gravity of this point in completing the migration from the N-1 approach to novel security management strategies.

In the development stages of this work, we identified an additional societal cost component related to the loss of generating units from the system. As presented in the earlier parts of this paper, for the purposes of security management in real-time, this cost component should encapsulate the effect of the loss of any generating unit on the continuity of supply further than the period of interest. Having established in this paper the scope for considering such a factor in the decision making process, we thus raise the necessity of accurately quantifying this value.

As already mentioned, the quantitative results presented in this paper are not based on validated reference values for the aforementioned cost components. To the best of the authors' comprehension, this remains in complete accordance with the purpose of establishing the fundamental properties of the proposed framework.

3) Developing Tractable Solution Algorithms for Large-Scale Power Systems: In parallel to the issues discussed in the preceding paragraphs, we should re-state that the exact solution of the optimization problem considered in this paper in large-scale power systems is a challenging task in terms of computational complexity. In the next steps of this work we intend to consider:

- Re-casting the problem under consideration in the AC power flow context. In this context, we aim not only to enhance the representation of the system behavior but also to extend the set of potential corrective control actions beyond the set adopted in the development of the present work. Recent works from the applied mathematics community, providing admissible convex relations of the AC OPF may show to be useful in this context [20].
- Defining approximations of the cost function (4) on the basis of the scenario tree approach from the multi-stage stochastic programming literature [21].
- Replacing the chance constraint (3) by an appropriate number of hard constraints defined over a sample of scenarios drawn according to the probabilistic model of our problem, building on the recent results given in [22], [23].
- Identifying a well-chosen subset of the combinations of contingencies and behaviors that have to be taken into account as credible events in order to warrant the system security level. We note that the starting point for the formulation of such a subset extends beyond the set of events considered under the N-1 approach (*i.e.* the failure of any single system component) to encapsulate all the possible events according to the vulnerability of the system components.
- Evaluating the performance of the proposed framework on a large-scale power system with respect to the N-1 approach, as implemented in today's practice by TSOs. To that end, we will exclude the consideration of the probability of occurrence of the various credible contingencies from the model of the N-1 approach.

4) Extension to Alternative Decision Making Horizons: As a final point, we return to the multi-stage nature of the

power system security management problem. The consideration of the latest decision stage in this work, serves as a first step toward developing a coherent approach across the full set of the overlapping decision making horizons.

To that end, we suggest to gradually extend this research by working backwards, from real-time to intraday and day-ahead operation planning, then maintenance management, then system expansion. Notice that by doing so the space of uncertainties to be modelled and the space of decisions to be jointly optimised will have to be gradually expanded.

In particular, as soon as we reach the operation planning stage, one major additional source of uncertainty to be accounted for are the power injections assumed from renewable generation, demand, and market driven dispatchable generation units.

Acknowledgements

Appendix A

The present appendix outlines the linearization of products of binary and continuous variables appearing in the formulation presented in section III. More specifically, equalities (29) and (32) involve products of binary variable $\lambda_\ell^c(b)$ and free continuous variable $\hat{\theta}_n^c(b)$ as in,

$$\hat{f}_\ell^c(b) - \frac{a_\ell^c \cdot (1 - \lambda_\ell^c(b))}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \hat{\theta}_n^c(b) = 0 \tag{44}$$

$$\hat{f}_\ell^c(b) - \frac{a_\ell^c \cdot (1 - \tau_c \cdot \lambda_\ell^c(b))}{X_\ell} \sum_{n \in \mathcal{N}_n} \beta_{n,\ell} \cdot \hat{\theta}_n^c(b) = 0. \tag{45}$$

The product $\lambda_\ell^c(b) \cdot \hat{\theta}_n^c(b)$ can be replaced by free continuous variable $\tilde{\theta}_n^c(b)$ via the following set of constraints:

$$\tilde{\theta}_n^c(b) \leq \lambda_\ell^c(b) \cdot M \tag{46}$$

$$\tilde{\theta}_n^c(b) \geq -\lambda_\ell^c(b) \cdot M \tag{47}$$

$$\tilde{\theta}_n^c(b) - \hat{\theta}_n^c(b) \leq (1 - \lambda_\ell^c(b)) \cdot M \tag{48}$$

$$\tilde{\theta}_n^c(b) - \hat{\theta}_n^c(b) \geq (\lambda_\ell^c(b) - 1) \cdot M. \tag{49}$$

Inequalities (36) through (39) involve products of binary variable $y_g^c(b)$ and non-negative continuous variables P_g^0, P_g^c as in,

$$\hat{P}_g^c(b) - (1 - y_g^c(b)) \cdot P_g^c \leq 0 \tag{50}$$

$$-\hat{P}_g^c(b) + (1 - y_g^c(b)) \cdot (P_g^c - a_g^c \cdot \Delta P_g^e) \leq 0 \tag{51}$$

$$\hat{P}_g^c(b) - a_g^c \cdot (1 - y_g^c(b)) \cdot P_g^0 \leq 0 \tag{52}$$

$$-\hat{P}_g^c(b) + a_g^c \cdot (1 - y_g^c(b)) \cdot (P_g^0 - \Delta P_g^e) \leq 0. \tag{53}$$

The product $y_g^c(b) \cdot P_g^0$ can be replaced by non-negative continuous variable $\tilde{P}_g^0 \geq 0$ through[13]:

$$\tilde{P}_g^0 \leq y_g^c(b) \cdot M \tag{54}$$

$$\tilde{P}_g^0 - P_g^0 \leq (1 - y_g^c(b)) \cdot M \tag{55}$$

$$\tilde{P}_g^0 - P_g^0 \geq (y_g^c(b) - 1) \cdot M. \tag{56}$$

Appendix B

The MILP formulation of (7)-(43) may be extended in a straightforward way to piece-wise linear costs functions instead of the objective (7). In the present appendix we explain how this may be exploited to adopt a different objective function, according to an incremental settlement of preventive and/or corrective control costs.

Preventive Control Adjustment Cost

In some regulatory jurisdictions, a TSO would only be liable for the cost of deviations with respect to the outcome of an already settled market clearing, denoted henceforth as P_g^M for every unit $g \in \mathcal{N}_g$. In order to model this, in the general case wherein different fees are applicable to upwards or downwards changes, the first term of (7) would be modified in the following way:

$$C_0(x_0, u_0) = \left(\sum_g \overline{c}_g \cdot \overline{P}_g^M + \sum_g \underline{c}_g \cdot \underline{P}_g^M \right), \tag{57}$$

where symbols $\overline{c}_g$ and $\underline{c}_g$ denote the per unit costs of upwards and downwards deviations respectively and:

$$\overline{P}_g^M = \max \left\{ (P_g^0 - P_g^M), 0 \right\} \tag{58}$$

$$\underline{P}_g^M = \max \left\{ (P_g^M - P_g^0), 0 \right\}. \tag{59}$$

The expression of (58) and (59) in a linear form can be made by the use of a set of logical constraints. We also notice that the case wherein deviations are remunerated according to an absolute value (*i.e.* $|P_g^M - P_g^0|$) is a particular case of (57)-(59) where $\overline{c} = \underline{c}_g$.

Corrective Control Adjustment Cost

A commonly used alternative for the costs of corrective control penalises any modification against the preventive schedule. In a similar manner to (57)-(59), this can be integrated in the MILP of (7)-(43) via:

$$C_c(x_0, u_0, c, u_c) = \left(\sum_g \overline{c}_g^r \cdot \overline{P}_g^c + \sum_g \underline{c}_g^r \cdot \underline{P}_g^c \right), \tag{60}$$

where symbols $\overline{c}_g^r$ and $\underline{c}_g^r$ denote the per unit costs of incremental/decremental deviations respectively, while:

$$\overline{P}_g^c = \max \left\{ (P_g^c - P_g^0), 0 \right\} \tag{61}$$

$$\underline{P}_g^c = \max \left\{ (P_g^0 - P_g^c), 0 \right\}. \tag{62}$$

[13]The same process is applied to replace the product $y_g^c(b) \cdot P_g^c$ by non-negative continuous variable $\tilde{P}_g^c \geq 0$.

References

[1] L. Wehenkel, "Emergency control and its strategies," in *Proceedings of the 13th Power Systems Computation Conference, PSCC99*, pp. 35–48.

[2] P. Panciatici, Y. Hassaine, S. Fliscounakis, L. Platbrood, M. Ortega-Vazquez, J. Martinez-Ramos, and L. Wehenkel, "Security management under uncertainty: from day-ahead planning to intraday operation," in *Bulk Power System Dynamics and Control-VIII, IREP Symposium*, pp. 1–8, IEEE, 2010.

[3] P. Varaiya, F. Wu, and J. Bialek, "smart operation of smart grid: risk-limiting dispatch," *Proceedings of the IEEE*, vol. 99, no. 11, pp. 40–57, 2011.

[4] F. Capitanescu, S. Fliscounakis, P. Panciatici, and L. Wehenkel, "Day-ahead security assessment under uncertainty relying on the combination of preventive and corrective controls to face worst-case scenarios," in *Proceedings of PSCC*, 2011.

[5] F. Capitanescu, J. Martinez Ramos, P. Panciatici, D. Kirschen, A. Marano Marcolini, L. Platbrood, and L. Wehenkel, "State-of-the-art, challenges, and future trends in security constrained optimal power flow," *Electric Power Systems Research*, vol. 81, no. 8, pp. 1731–1741, 2011.

[6] M. Vrakopoulou, K. Margellos, J. Lygeros, and G. Andersson, "Probabilistic guarantees for the n-1 security of systems with wind power generation," in *Proceedings of PMAPS*, 2012.

[7] A. Patton, "A probability method for bulk power system security assessment: I-basic concepts," *Power Apparatus and Systems, IEEE Transactions on*, no. 1, pp. 54–61, 1972.

[8] A. Patton, "A probability method for bulk power system security assessment: II-development of probability models for normally-operating components," *Power Apparatus and Systems, IEEE Transactions on*, no. 6, pp. 2480–2485, 1972.

[9] A. Patton, "A probability method for bulk power system security assessment: III-models for stand-by generators and field data collection and analysis," *Power Apparatus and Systems, IEEE Transactions on*, no. 6, pp. 2486–2493, 1972.

[10] F. Bouffard, F. Galiana, and A. Conejo, "Market-clearing with stochastic security-part I: formulation," *Power Systems, IEEE Transactions on*, vol. 20, no. 4, pp. 1818–1826, 2005.

[11] R.-C. Dai, H. Pham, Y. Wang, and J. D. McCalley, "Long-term benefits of online risk-based direct-current optimal power flow," *Proceedings of the Institution of Mechanical Engineers, art O: Journal of Risk and Reliability*, vol. 226, no. 1, pp. 65–74, 2012.

[12] J. McCalley, S. Asgarpoor, L. Bertling, R. Billinton, H. Chao, J. Chen, J. Endrenyi, R. Fletcher, A. Ford, C. Grigg, G. Hamoud, D. Logan, A. Meliopoulos, M. Ni, N. Rau, L. Salvaderi, M. Schilling, Y. Schlumberger, A. Schneider, and C. Singh, "Probabilistic security assessment for power system operations," in *Power Engineering Society General Meeting, 2004. IEEE*, pp. 212–220 Vol.1, 2004.

[13] F. Yang, A. Meliopoulos, G. Cokkinides, and Q. Binh Dam, "Bulk power system reliability assessment considering protection system hidden failures," in *Bulk Power System Dynamics and Control - VII. Revitalizing Operational Reliability, 2007 iREP Symposium*, pp. 1–8, 2007.

[14] A. J. Wood and B. F. Wollenberg, *Power Generation, Operation, and Control*. New York: Wiley Interscience, second ed., 1996.

[15] F. Bouffard, F. D. Galiana, and A. J. Conejo, "Market-clearing with stochastic security-part II: case studies," vol. 20, pp. 1827–1835, Nov. 2005.

[16] R. Billinton and R. N. Allan, *Reliability Evaluation of Power Systems*. New York: Plenum, second ed., 1996.

[17] D. Kirschen and D. Jayaweera, "Comparison of risk-based and deterministic security assessments," *Generation, Transmission Distribution, IET*, vol. 1, no. 4, pp. 527–533, 2007.

[18] P. Linares and L. Rey, "The costs of electricity interruptions in Spain. are we sending the right signals?," working papers, Economics for Energy, Apr. 2012.

[19] E. Leahy and R. S. Tol, "An estimate of the value of lost load for Ireland," *Energy Policy*, vol. 39, no. 3, pp. 1514 – 1520, 2011.

[20] J. Lavaei and S. Low, "Zero duality gap in optimal power flow problem," *IEEE Transactions on Power Systems*, vol. 27, no. 1, pp. 92–107, 2012.

[21] B. Defourny, D. Ernst, and L. Wehenkel, "Scenario trees and policy selection for multistage stochastic programming using machine learning," *INFORMS Journal on Computing*, 2012.

[22] M. Campi and S. Garatti, "The exact feasibility of randomized solutions of uncertain convex programs," *SIAM journal of optimization*, vol. 19, no. 3, pp. 1211–1230, 2008.

[23] M. Campi and S. Garatti, "A sampling-and-discarding approach to chance-constrained optimization: feasibility and optimality," *J Optim Theory Appl*, vol. 148, pp. 257–280, 2011.