J. Mod. Power Syst. Clean Energy (2018) 6(5):930–943
https://doi.org/10.1007/s40565-018-0447-8

Risk-based method to secure power systems against cyber-physical faults with cascading impacts: a system protection scheme application

Jose Luis CALVO[1], Simon H. TINDEMANS[2], Goran STRBAC[1]

Abstract The utilization levels of the transmission network can be enhanced by the use of automated protection schemes that rapidly respond to disturbances. However, such corrective systems may suffer from malfunctions that have the potential to exacerbate the impact of the disturbance. This paper addresses the challenge of jointly optimizing the dispatch of generators and protection settings in this context. This requires a holistic assessment of the cyber (protection logic) and physical (network) systems, considering the failures in each part and their interplay. Special protection schemes are used as a prototypical example of such a system. An iterative optimization method is proposed that relies on power system response simulations in order to perform detailed impact assessments and compare candidate solutions. The candidate solutions are generated on the basis of a security-constrained dispatch that also secures the system against a set of cyber failure modes. A case study is developed for a generation rejection scheme on the IEEE reliability test system (RTS): candidate solutions are produced based on a mixed integer linear programming optimisation model, and loss-of-load costs are computed using a basic cascading outage algorithm. It is shown that the partial security approach is able to identify solutions that provide a good balance of operational costs and loss-of-load risks, both in a fixed dispatch and variable dispatch context.

Keywords Power system operations, Cyber-physical systems, Reliability, System protection schemes, Risk-aware dispatch

CrossCheck date: 31 July 2018

Received: 2 December 2017 / Accepted: 31 July 2018 / Published online: 12 September 2018

✉ Simon H. TINDEMANS
s.h.tindemans@tudelft.nl

Jose Luis CALVO
j.calvo10@imperial.ac.uk

Goran STRBAC
g.strbac@imperial.ac.uk

[1] Department of Electrical and Electronic Engineering, Imperial College London, London SW7 2AZ, UK

[2] Department of Electrical Sustainable Energy, Delft University of Technology, Mekelweg 4, 2628 CD Delft, The Netherlands

1 Introduction

The electricity grid is primarily recognized as a physical transport layer for electrical energy. However, modern power systems are increasingly reliant on sensing, communication, computing and automated control to deliver the efficiency, flexibility and reliability that is required of them. They should therefore be understood as cyber-physical systems (CPSs) [1], where system-level behaviour results from the interplay between physical processes, information flows and control actions. A particular challenge is presented by the fact that power systems are critical infrastructures, where an inability to deliver energy to end users comes at a very high cost. This makes the study of failure modes in cyber-physical energy system particularly pressing. Although the need for such analysis has been recognized [1, 2], the development of formal reliability models for cyber-physical energy system is still at an early stage [3, 4].

System protection schemes (SPSs), also known as remedial action schemes (RASs) or system integrity protection schemes (SIPSs), are a natural candidate for studying CPS reliability in a well-defined context. SPSs are designed to detect abnormal power system conditions and initiate predetermined corrective actions to mitigate their impact [5]. SPS interventions include changes in load, generation, or system topology; these are usually triggered by the remote detection of contingencies, mediated by information communications technology (ICT) infrastructure. In other words, events originate in the physical domain (initiating contingencies), traverse the cyber domain (control logic and signals) and return to the physical domain (interventions in the power system).

The use of SPS has been largely associated with last-resort defense plans [6]. As such, SPS helps to protect the power system from high-impact low-probability events, including cascading outages. Alternatively, SPS can be used to improve the utilisation levels of electricity networks, alleviating operational security constraints in network-constrained areas. The principle is simple: SPSs take corrective actions upon the occurrence of a network contingency to avoid overloading the remaining circuits. In this second application, SPS helps to reduce generation dispatch costs, for example when large amounts of remote renewable resources are connected to the grid: preventive security constraints may require costly curtailments of renewable generation and dispatching generators out of merit [7]. On the other hand, activation of an SPS incurs additional operational costs, for example in the form of availability and utilization payments and potential loss-of-load costs [4]. The resulting cost-benefit problem falls into the security constraint optimal power flow (SCOPF) general framework [8] with the further aim of considering the value of the corrective security [9]. Significant research has been dedicated to resolve variations of this problem [10, 11] which show the need to consider these corrective systems in a cost-benefit fashion. The benefits from SPS have been recently explored in a multi-area electricity market system where a supra-operator determines the optimal power flows between areas [12].

As a result of these benefits, there is growing interest in SPS deployment of in the benefits from SPS deployment as noted in a survey by IEEE and PSERC [5] on global experiences with such systems, and other recent examples [13–15]. However, history has shown that SPSs are not always dependable: [16] reviewed NERC system disturbance reports from 1986-2009 and found that of 26 SPS malfunctions, 11 cases were related to ICT operational failures. The perceived risk associated with these systems has been highlighted already in 1996, when a IEEE-CIGRE survey to the power industry [17] estimated costs related to SPS failures to be very high. Given the potentially large impact of such malfunctions, it is critical to develop an understanding of the link between cyber-failures and overall system reliability.

A number of modelling techniques have been proposed and investigated in this area [18]. Examples of SPS risk modelling with the aim of computing optimal arming points for generation rejection schemes are found in [19, 20]. Similar reliability models have been proposed for digital substations [21], resulting in proposals for generic representations of cyber-physical fault pathways, such as the cyber-physical interface matrix [22] and the consequent event matrix [3]. The IEEE Task Force on Reliability Considerations in Emerging Cyber-Physical Energy Systems has recently compiled the state of the art in this research area [23].

The role of SPS in improving economic utilisation of electricity networks necessitates a wider view of SPS reliability. The operator should ideally embed the notion of SPS reliability into its operational decisions about protection settings, generator dispatch and the loading of transmission lines. The main challenge in this exercise is that the outcomes from SPS malfunctions are often highly nonlinear, for example when the malfunction triggers a cascading outage. Hence, when it has been attempted at all, a joint cost-benefit analysis of dispatch and protection settings has typically relied on simplified representation of SPS malfunction and the resulting system response, e.g. [7]. A more elaborate SPS model was used in [4], but the simplicity of the system ensured that all failure pathways were readily enumerated.

This paper presents a method to embed SPS reliability aspects into optimal operational decisions with an explicit allowance for the evaluation of complex consequences of faults - cascading outages in particular. First, Section 2 formally defines the problem the operator faces when co-optimizing economic dispatch and the configuration of protection systems. Then, Section 3 describes an iterative approach to find an approximate solution to this problem, which builds on the concept of partial security scenarios introduced in [4] to generate plausible candidate solutions in a very large parameter space. Starting from the initial assumption that the cyber system works as designed, the method iteratively secures the system against a growing set of cyber-failure modes and evaluates the results obtained, thus balancing the cost of protection against the risks due to malfunctions that are not explicitly secured. The method uses explicit cascading outage simulations to compute costs associated with operational decisions such as dispatch of generators, SPS configurations and reserve deployment. An illustration of the method on the 24-bus IEEE reliability test system (RTS) is presented in Section 4, along with its specific power system and operational decision models. The results in Section 5 suggest a robust ability to identify solutions that better balance costs of supply, protection and interruption, compared to alternative approaches. The findings are further supported by results on the two-area RTS.

2 Problem statement and challenges

We consider the problem of optimal system operation from the perspective of a central operator that wishes to secure the network against a set of contingencies $\mathcal{C}$. The following sequence of events is assumed [4]: ① in response to a given demand pattern and availability of generators, a generation and reserve dispatch is determined and, when desirable, the SPS is configured and armed; ② contingencies occur with a certain probability; ③ a contingency may trigger an SPS response and/or activation of frequency response to balance the system; ④ if residual constraint violations are present (DC overloads in the context of this paper), this results in further automated protection action, e.g. branch openings, that may cause loss of supply for customers. Note that the operator has no recourse after a contingency occurs, so that the dispatch and protection configuration fully define the system's response to contingencies.

The operator can choose to secure the system in a preventive manner, by adjusting the pre-fault generator dispatch, or in a corrective manner, by relying on automated post-fault automatic actions to return the system within operational limits. However, as these corrective actions may fail, they are accompanied by a risk of adverse consequences. The optimal decision is a trade-off between security and profitability based on a quantitative assessment of risk. Notably, in many real-world systems the system operator does not autonomously dispatch the generation assets, but relies on the markets to do so. Nevertheless, the system operator would still configure protection settings and influence reserve allocation, and it may adjust proposed market positions based if this is warranted by system security. Moreover, knowledge of the optimal solution obtained by a central operator, even if it cannot always be implemented in practice, may serve to identify shortcomings in markets or regulatory designs.

Formally, the operational problem of securing the system consists of choosing a generator dispatch and a configuration of the protection system. We denote the sets of related decision variables by $\mathcal{D}$ and $\mathcal{S}$, respectively. For the analysis, the set of credible contingencies $\mathcal{C}$ is divided into two classes: contingencies that are connected to a protection system thus may trigger a protection response ($\mathcal{C}_p$) and those that do not ($\mathcal{C}_n$). The contingencies in $\mathcal{C}_n$ are secured in a preventive manner and those in $\mathcal{C}_p$ are configured to trigger the protection system. For those contingencies a quantitative risk trade-off is made, which explicitly accounts for possible failures of the protection system.

The contingencies $c \in \mathcal{C}_p$ are assumed to occur with a rate λ_c within the operational period under consideration. For each initiating contingency c, there is one intended 'design outcome' $o(c)$ of the protection system, but in practice the initiating contingency can result in a range of protection system outcomes $\mathcal{O}$. If a probabilistic model is available for the failures within the cyber system, this results in a set of conditional probabilities $p_{o|c}$ for outcomes o, depending on the initiating contingency c, with $\sum_{o \in \mathcal{O}} p_{o|c} = 1$. This set of conditional probabilities, also used in [4], encodes the same information as the cyber-physical interface matrix (CPIM) [22]. We further define the concept of a cyber-physical post-fault scenario $q \equiv (c, o)$, which consists of an initiating contingency c and a subsequent protection outcome o. The rate of occurrence μ_q of each outcome $q \in (\mathcal{Q}_p \times \mathcal{O})$ is given by $\mu_q = \lambda_c \times p_{o|c}$.

The operator's cost-benefit optimization for an operational window Δt is then expressed as:

$$\begin{aligned} \min_{\mathcal{D},\mathcal{S}} [G + P + X] \equiv \min_{\mathcal{D},\mathcal{S}} \{ & G(\mathcal{D}) + P^a(\mathcal{D}, \mathcal{S}) \\ & + \Delta t \sum_{c \in \mathcal{C}_p, o \in \mathcal{O}} \lambda_c p_{o|c} [P^u(\mathcal{D}, \mathcal{S}, c, o) \\ & + L(\mathcal{D}, \mathcal{S}, c, o)]\} \end{aligned} \tag{1}$$

s.t.

$$\begin{cases} h(\mathcal{D}, \mathcal{S}, \mathcal{C}, \mathcal{O}) \leq 0 \\ g(\mathcal{D}, \mathcal{S}, \mathcal{C}, \mathcal{O}) = 0 \end{cases} \tag{2}$$

where G, P, X are generation, protection and loss-of-load costs, respectively. The protection costs P consist of a deterministic availability fee $P^a(\mathcal{D}, \mathcal{S})$ and a per-event utilization fee $P^u(\mathcal{D}, \mathcal{S}, c, o)$ that depends on the CPS scenario (c, o). The loss-of-load risk X represents the expected cost associated with loss of supply to end users, consisting of per-event loss contributions $L(\mathcal{D}, \mathcal{S}, c, o)$. These loss contributions are determined, for example, by computation of the energy not supplied and an estimated value of lost load (VoLL). The constraints (2) contain pre-fault and post-fault constraints for all scenarios, including those in the security-constrained contingency set $\mathcal{C}_n$ (see e.g. [8]).

In [4], the problem (1) was solved explicitly for an SPS in a very simple network. However, in a general setting, the computation of the load-shedding cost L requires detailed analysis of a complex power system. The costs may, for example, depend on the outcome of a multi-stage cascading process. When complex failure dynamics are present, the loss-of-load cost $L(\mathcal{D}, \mathcal{S}, c, o)$ cannot be expressed algebraically as a function of $\mathcal{D}$ and $\mathcal{S}$. In this case, the impact can only realistically be evaluated by explicit simulation of individual events and operating points.

3 Partial security method

In the following, we describe an heuristic approach to find an approximate solution to (1). The risk term X, which cannot be evaluated within a symbolic optimization, is replaced by an additional set of constraints. These constraints are varied to yield a set of candidate solutions, the best of which is selected by enumeration and direct simulation. The method consists of three parts that are described in detail below, and summarized in Fig. 1.

3.1 Selection among candidate solutions

At a high level, the optimization is implemented as an enumeration across a set of 'candidate solutions'. Let $\mathcal{K} = \{\kappa_1, \kappa_2, \ldots, \kappa_N\}$ be a set of candidate solutions $\kappa_i \equiv (\mathcal{D}_i, \mathcal{S}_i)$ (to be defined below). The optimization then takes the form

$$\kappa^* = \underset{\kappa \in \mathcal{K}}{\operatorname{argmin}}\, G(\kappa) + P(\kappa) + X(\kappa) \tag{3}$$

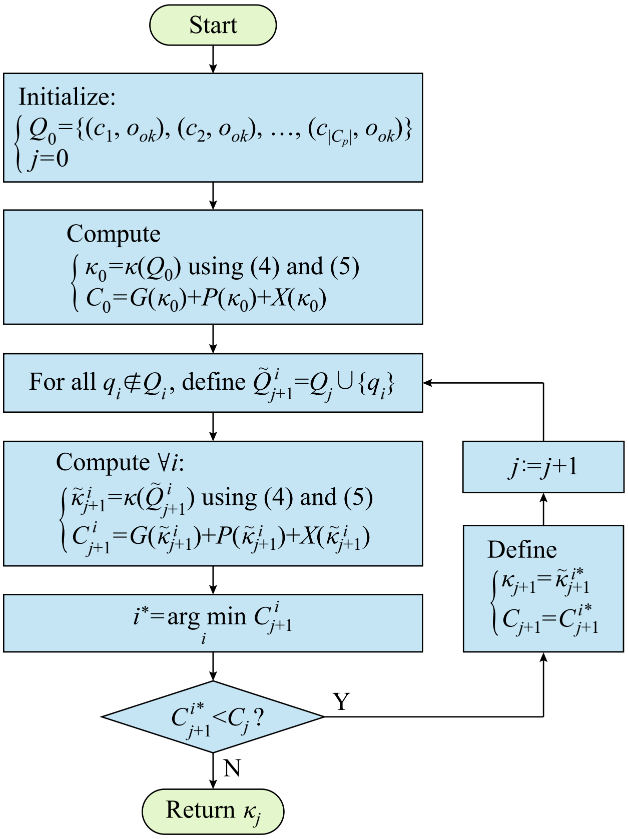
Start
Initialize:
Q_0={(c_1, o_{ok}), (c_2, o_{ok}), …, ($c_{|C_p|}$, o_{ok})}
j=0
Compute
κ_0=κ(Q_0) using (4) and (5)
C_0=G(κ_0)+P(κ_0)+X(κ_0)
For all $q_i \notin Q_i$, define $\tilde{Q}^i_{j+1}$=$Q_j \cup \{q_i\}$
Compute ∀i:
$\tilde{\kappa}^i_{j+1}$=κ($\tilde{Q}^i_{j+1}$) using (4) and (5)
C^i_{j+1}=G($\tilde{\kappa}^i_{j+1}$)+P($\tilde{\kappa}^i_{j+1}$)+X($\tilde{\kappa}^i_{j+1}$)
i^*=arg min$_i$ C^i_{j+1}
C^{i*}_{j+1}<C_j?
Y
N
Return κ_j
j:=j+1
Define
κ_{j+1}=$\tilde{\kappa}^{i*}_{j+1}$
C_{j+1}=C^{i*}_{j+1}

Fig. 1 Process for computation of partial security solution to reduce operational costs

For each of the candidate solutions, all protection system outcome scenarios are enumerated explicitly, contributing according to their probability of occurrence. The load-shedding impact may be computed by means of simulation, or using an independent optimization procedure. This point-by-point analysis guarantees that the best candidate is selected from the set $\mathcal{K}$.

3.2 Partial security candidates

The challenge is thus transformed to the generation of a suitable candidate set $\mathcal{K}$. A heuristic approach to generate suitable candidates using a generalized SCOPF formulation is described below.

Reference [4] studied an unreliable SPS in a small demonstration system, where (1) could be solved directly. It was observed that the optimal SPS configuration is always a configuration that just prevents cascading overloads in one of the outcome scenarios. In other words, the system is operated such that for a particular combination of an initiating contingency and SPS failure mode, one or more of the components are at their operational threshold (e.g. thermal limit). This is intuitive, because crossing these thresholds is associated with further disconnections and possible customer disconnections. In the studied model, the optimal solution was therefore always one of a discrete set of 'candidate solutions' that were directly related to the triggering contingencies and associated SPS outcomes.

In the present paper, we postulate that the same principle can be applied more generally to generate potentially optimal solutions to (1). We define partial security configurations as solutions that are guaranteed to prevent load shedding for one or more scenarios $q = (c, o)$. A partial security configuration for the set $\mathcal{Q} = \{q_1, q_2, \ldots, q_k\}$ is defined as a solution that has no post-contingency constraint violations and thereby necessarily prevents load-shedding for all scenarios in $\mathcal{Q}$. This is enforced by a set of constraints $h_\mathcal{Q}(\mathcal{D}, \mathcal{S}, \mathcal{C}, \mathcal{O}) \leq 0, g_\mathcal{Q}(\mathcal{D}, \mathcal{S}, \mathcal{C}, \mathcal{O}) = 0$. Simultaneously we remove the load-shedding risk X from the objective function.

A practical concern is that the protection configuration itself (the decision variables $\mathcal{S}$) impacts its possible failure modes, and therefore the possible elements of $\mathcal{Q}$. Deciding $\mathcal{S}$ on the basis of a given set of failure pathways $\mathcal{Q}$ reverses this causality: it effectively makes the optimizer clairvoyant, letting it avoid those protection elements that fail in some scenario $q \in \mathcal{Q}$. For example, in the context of a generation rejection scheme (an SPS that disconnects generation in abnormal system conditions), each outcome o is characterized by a collection of generators that successfully disconnect. Without further restrictions the partial security constraints $h_{\mathcal{Q}}$ would simply result in the use of generators that will not be impacted by the failures. To rectify this issue, we introduce the constraint $\mathcal{S} \in \Sigma(\mathcal{Q})$ that ensures that the valid choices of protection configuration are those that are actually affected by the scenarios in $\mathcal{Q}$.

Summarizing the above, the partial security configuration for a set of scenarios $\mathcal{Q}$ is defined as:

$$\kappa(\mathcal{Q}) = \underset{\mathcal{D},\mathcal{S}}{\operatorname{argmin}} \Bigg[G(\mathcal{D}) + P^a(\mathcal{D},\mathcal{S}) + \Delta t \sum_{c,o} \lambda_c p_{o|c} P^u(\mathcal{D},\mathcal{S},c,o) \Bigg] \tag{4}$$

s.t.

$$\begin{cases} h(\mathcal{D},\mathcal{S},\mathcal{C},\mathcal{O}) \le 0 \\ g(\mathcal{D},\mathcal{S},\mathcal{C},\mathcal{O}) = 0 \\ h_{\mathcal{Q}}(\mathcal{D},\mathcal{S},\mathcal{C},\mathcal{O}) \le 0 \\ g_{\mathcal{Q}}(\mathcal{D},\mathcal{S},\mathcal{C},\mathcal{O}) = 0 \\ \mathcal{S} \in \Sigma(\mathcal{Q}) \end{cases} \tag{5}$$

This is effectively an SCOPF formulation that secures the system against the set of non-SPS-triggering contingencies $\mathcal{C}_n$ and the set of contingency-outcome pairs in $\mathcal{Q}$.

3.3 Iterative set expansion

The techniques from Sections 3.1 and 3.2 can be combined into an intuitive heuristic search algorithm as follows. Consider the set of all possible outcome scenarios $\overline{\mathcal{Q}}$, obtained by combining all protected contingencies $\mathcal{C}_p$ with all possible protection outcomes $\mathcal{O}$. Partial security sets $\mathcal{Q}_i$ can be generated to represent all possible subsets of $\overline{\mathcal{Q}}$, resulting in a full set of partial security candidates $\{\kappa_i\}$. In theory, the best of these candidates can be selected through explicit simulation and enumeration, using (3). However, this naive approach is impractical in practice, because the full number of partial security scenarios equals $2^{|\mathcal{C}_p| \times |\mathcal{O}|}$, making it infeasible to evaluate all candidates for even moderately large systems.

To address this challenge, a further heuristic is proposed that relies on two further simplifications:

1) Consider only protection outcomes involving at most one component malfunction (an $N-1$ search of cyber failures). This greatly reduces the size of the set $\mathcal{O}$.
2) Rather than an exhaustive search, sequentially enlarge the partial security set $\mathcal{Q}_i$ using a steepest descent algorithm.

The algorithm is depicted in Fig. 1, and described below.

The algorithm starts with the set $\mathcal{Q}_0$ that contains all scenarios corresponding to correct SPS operation: one scenario for each contingency, paired with the outcome o_{ok} in which the SPS operates correctly. The corresponding candidate solution $\kappa_0 = \kappa(\mathcal{Q}_0)$ reflects the assumption that the SPS is dependable.

Next, the set of secure scenarios is expanded in an iterative fashion. The initial set $\mathcal{Q}_0$ is combined sequentially with each single credible SPS failure scenario to generate trial sets $\tilde{\mathcal{Q}}_1^i$, where i runs over all included failure scenarios. Partial security candidates $\tilde{\kappa}_1^i$ are generated for each trial set and the best candidate is selected through enumeration and explicit simulation, according to (3). The winning candidate solution and its corresponding secure scenario set are labeled κ_1 and $\mathcal{Q}_1$, respectively. In case of multiple best candidates, the method decides on a 'first come first served' basis: selecting the first candidate that attains the local optimum. The process proceeds analogously in subsequent stages: single credible failure scenarios are added to $\mathcal{Q}_1$ to generate $\tilde{\mathcal{Q}}_2^i$ and associated candidate solutions $\tilde{\kappa}_2^i$, and the winning candidate solution is denoted by κ_2. This algorithm continues until the objective function of κ_{j+1} at iteration $j+1$ ceases to improve on the previous iteration κ_j.

The procedure above describes a greedy approach to exploring the search space defined by the constraint $\mathcal{Q} \subseteq \overline{\mathcal{Q}}$, which is shown to work well in the examples in Section 5. However, the presented approach can readily be extended to use more elaborate heuristic search strategies, such as evolutionary algorithms.

4 Application: SPS IEEE RTS system

In this section, the partial security methodology for cyber-physical risk optimization described in Section 3 is specialized for a particular application to a SPS [5] on the basis of a generation rejection approach. Although the SPS is far from the most general example of a cyber-physical system, its extensive configurability, the inclusion of nonlocal actions and the far-reaching consequences of malfunctions make it a good demonstration case for the reliability of cyber-physical systems.

4.1 System description

The example is based on the IEEE RTS [24], shown in Fig. 2. To diversify the generation resources in the IEEE RTS, we divide the two original generators of 400 MW at Buses 18 and 21 in two separate units with capacities of

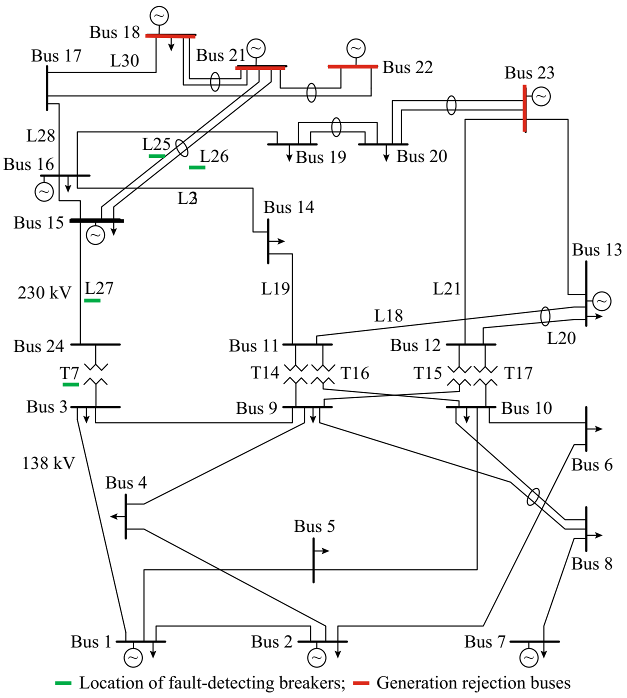

Fig. 2 IEEE reliability test system

160 MW and 240 MW (Bus 18) and 110 and 290 MW (Bus 21) respectively. We also reduce the capacity of all transmission lines by 5% in order to create additional stress in the network.

The set of relevant contingencies $\mathcal{C}$ is generated by considering the set of $N-d$ contingencies: single and double line outages. Line outages that immediately result in islanding are ignored. The system operator must also ensure a minimum requirement of reserve capacity to counteract the loss of the biggest generating unit in the network. We assume that 4% of the demand at each bus is available to provide reserve services. The price of reserve availability is assumed to be $\pi^{a} = 30\,\text{\$/MWh}$. The price of generation disconnection by the SPS is $\pi^{u} = 1000\,\text{\$/MW}$ event and VoLL is $30000/MWh. Other costs are derived from the Matpower RTS case [25]; linear generating costs are obtained through linear interpolation between the minimum and maximum generation levels.

The network is characterized by dominant north-south power flows as the cheapest generating units are located at exporting Buses 18, 21, 22 and 23 shown in Fig. 2. To reduce generation curtailment in the north area, a generation rejection SPS is installed to detect and respond to faults on line 27 (L27) and in transformer 7 (T7) as well as to double circuit faults in lines 25 and 26. Any of these faults will trigger SPS activation resulting in the immediate disconnection of remote generators and, through system rebalancing, a corresponding activation reserves elsewhere in the system. The system operator configures the SPS by pre-selecting generators from Buses 18, 21, 22 and 23 to trip in response to the detection of one of the three triggering contingencies. It is assumed that SPS-connected generators are must-run units and do not provide reserve services. To simplify the problem representation and focus on relevant details, we do not distinguish between frequency response services and operating reserves, instead referring to both as reserves.

To simulate bad weather conditions the nominal outage rates [24], considering both permanent and transient outages, are multiplied by a factor of 15. The double circuit fault rate for lines 25 and 26 is taken to be 7.5% of the resulting outage rate of line 26. The resulting fault rates are $\lambda_7 = 3.43 \times 10^{-5}, \lambda_{27} = 0.0013$ and $\lambda_{25\cap 26} = 1.69 \times 10^{-4}$ (events/hour).

The SPS measurement and control logic constitutes the cyber-system that interfaces with the physical network at its inputs and outputs; a block model of its main components is shown in Fig. 3. In Fig. 3, the arrows on the left represent contingencies and the solid lines are the connections between functional blocks. A generator is tripped in response to a contingency if it is armed ($t_i = 1$) and all blocks between the initiating contingency and the generator are available. The SPS is composed of relays, a logic control, bus-to-bus communication systems and generator circuit breakers. The relays R_{1-3} are located at T7 and branches 25-27. If a local fault is detected, the relays notify the logic controller at bus 15 (LC_{15}). It will trigger the SPS

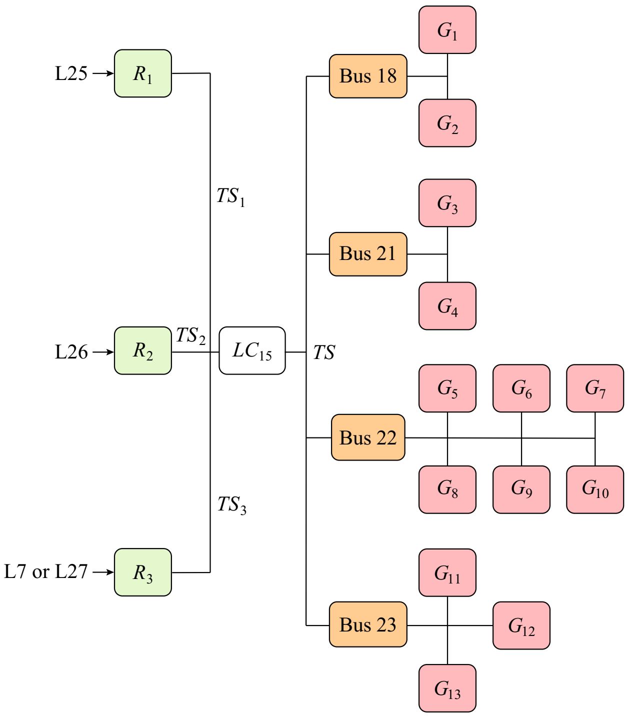

Fig. 3 Generation rejection SPS

response if it receives a signal from R_3 or from both R_1 and R_2 (because it is configured to respond to double line faults on lines 25 and 26). Triggering the response involves broadcasting a trip signal to connected generators G_{1-13} via the bus-specific communication channels $Bus\,x$. Figure 3 shows all available generators, but only those that have been 'armed' by the operator will actually receive the signal. For this simple SPS model, any of the triggering contingencies activates the same response.

The block diagram in Fig. 3 also represents the SPS reliability model. Each of the blocks can fail to operate on demand, resulting in a reduced dependability of the system. The reliability of each block is represented by its availability, and failures are assumed to be independent between blocks. The availability of relays, logic controller and generator circuit breakers is taken as $a_r = 0.9810, a_{lc} = 0.9925$ and $a_g = 0.9980$, respectively [4]. The availability of the communication channels to each bus is set to 0.9 to simulate a failure-prone environment. We note that the design dependability of real SPS is considerably higher, but this has not always been borne out in practice [16]. Moreover, as an example of an unreliable cyber-physical system it is illuminating to investigate this low-reliability regime. A further sensitivity study to this parameter is performed in Section 5.3.

The credible failure scenarios that are considered in the iterative optimization (Section 3.3) are those that affect a single generator (breaker failure), all generators at a bus (communication link failure) or the whole SPS (logic control and/or relay(s) failures). There are $|\mathcal{C}_p| \times (B + G + 1)$ such failure modes, where $|\mathcal{C}_p|$ is the number of SPS-triggering contingencies, B is the number of SPS-linked buses and G is the total number of generators connected to those buses. In practice, the number of relevant modes is further reduced by avoiding double-counting of failure modes involving identical generators at the same bus.

4.2 Generation of partial security solutions

In the following we develop the partial security formulation (4) for the specific case of the generation rejection scheme. In the following, subscripts i, n and l are used to refer to generators, nodes and lines, respectively. Superscripts are used to refer to the pre-fault scenario (0), an SPS outcome scenario ($q \in \mathcal{Q}$) or a preventively secured fault scenario ($k \in \mathcal{C}_n$).

The cost terms G, P^a and P^u are given by:

$$G(g) = \sum_{i \in \mathcal{G}} \alpha_i g_i \Delta t \tag{6}$$

$$P^a(r^g, r^d) = \pi^a \Delta t \left(\sum_{i \in \mathcal{G}} r_i^g + \sum_{n \in \mathcal{N}} r_n^d \right) \tag{7}$$

$$P^u(g, t, o) = \pi^u \sum_{i \in \mathcal{G}} q_{i|o} g_i t_i \tag{8}$$

The generation costs (6) are computed from the dispatch decision g_i and unit cost of energy of each generator (α_i) and the time step Δt. The availability fees for system protection services (7) are determined by the unit cost π^a (per MWh) and the amount of reserves provided by generators (r_i^g for generator i) and responsive demand (r_n^d in node n). The SPS utilization fees (8) consist of the unit cost π^u (per MW, per event) multiplied by the contribution of each generator i: the dispatch g_i is the reduction of output if the generator is successfully disconnected by the SPS, but this only happens if it has been selected to do so by the operator (t_i, binary) and if it is successfully triggered in the outcome scenario o ($q_{i|o}$).

Inserting (6)-(8), the problem (4) takes the form of a mixed integer linear programming (MILP) model.

$$\begin{aligned} \kappa(\mathcal{Q}) = \operatorname*{argmin}_{\mathcal{D},\mathcal{S}} \Delta t \Bigg[& \sum_{i \in \mathcal{G}} \alpha_i g_i + \pi^a \left(\sum_{i \in \mathcal{G}} r_i^g + \sum_{n \in \mathcal{N}} r_n^d \right) \\ & + \pi^u \sum_{c \in \mathcal{C}} \sum_{o \in \mathcal{O}} \sum_{i \in \mathcal{G}} \lambda_c p_{o|c} q_{i|o} t_i^* \Bigg] \end{aligned} \tag{9}$$

where

$$\begin{cases} t_i^* = g_i t_i \\ \mathcal{D} = \{u, g, r^g, r^d\} \\ \mathcal{S} = \{t\} \end{cases}$$

The dispatch decision $\mathcal{D}$ concerns the commitment (u_i, binary) and dispatch of generators (g_i) and reserve (r_i^g, r_n^d), and the protection decision $\mathcal{S}$ consists of the arming of generators to be tripped by the SPS (t_i, binary).

The constraints (5) of the abstract problem (4) are developed as follows. The nonlinear relation $t_i^* = g_i t_i$ for the total tripping capacity of generator i is replaced by the triplet of linear inequality constraints:

$$\begin{cases} g_i - t_i^* \le \overline{g}_i (1 - t_i) \\ t_i^* \le \overline{g}_i t_i \\ t_i^* \le g_i \end{cases} \tag{10}$$

The nodal power balance is enforced by the following equalities, which hold $\forall n \in \mathcal{N}$ (for all nodes), $\forall q \in \mathcal{Q}$ (all partial security scenarios), $\forall k \in \mathcal{C}_n$ (all preventively secured contingencies):

$$d_n = \sum_{i \in \mathcal{G}_n} g_i + A_{nl} f_l^0 \tag{11}$$

$$d_n = \sum_{i\in\mathcal{G}_n} g_i - \sum_{i\in\mathcal{GS}_n} q_{i|o} t_i^* + \sum_{i\in\mathcal{GR}_n} \Delta g_i^q + \Delta d_n^q + A_{nl} f_l^q \tag{12}$$

$$d_n = \sum_{i\in\mathcal{G}_n} g_i + A_{nl} f_l^k \tag{13}$$

where d_n is the nodal demand in node n, $\mathcal{G}_n$ are the indices of the local generators; those in $\mathcal{GS}_n$ may participate in the SPS and those in $\mathcal{GR}_n$ provide system reserves. The active power flow in line l is indicated by f_l, A_{nl} is the node-line incidence matrix (1 for incoming, -1 for outgoing) and Δg_i^q and Δd_n^q are the deployed reserves by generators and responsive demand, respectively, in node n and SPS outcome scenario q.

The DC power flow equations are completed by ($\forall l \in \mathcal{L}, \forall q \in \mathcal{Q}, \forall k \in \mathcal{C}_n$):

$$f_l^0 = \frac{1}{x_l} \sum_{n\in\mathcal{N}} A_{nl} \theta_n^0 \tag{14}$$

$$f_l^q = \begin{cases} 0 & \text{if } l \text{ is outaged in } c \\ \dfrac{1}{x_l} \displaystyle\sum_{n\in\mathcal{N}} A_{nl} \theta_n^q & \text{otherwise} \end{cases} \tag{15}$$

$$f_l^k = \begin{cases} 0 & \text{if } l \text{ is outaged in } k \\ \dfrac{1}{x_l} \displaystyle\sum_{n\in\mathcal{N}} A_{nl} \theta_n^k & \text{otherwise} \end{cases} \tag{16}$$

$$-\overline{f}_l \le f_l^0 \le \overline{f}_l \tag{17}$$

$$-\overline{f}_l \le f_l^q \le \overline{f}_l \tag{18}$$

$$-\overline{f}_l \le f_l^k \le \overline{f}_l \tag{19}$$

where $\overline{f}_l$ is the thermal limit of line l; x_l is its reactance and θ_n the phase angle of node n.

Constraints on active power dispatch and reserves are given by:

$$\begin{cases} \sum_{i\in\mathcal{GR}} r_i^g + \sum_{n\in\mathcal{N}} r_n^d \ge 350 \text{ MW} \\ \sum_{i\in\mathcal{GR}} r_i^g + \sum_{n\in\mathcal{N}} r_n^d \ge \sum_{i\in\mathcal{GS}} t_i^* \end{cases} \tag{20}$$

$$r_n^d \le 0.04 d_n \qquad \forall n \in \mathcal{N} \tag{21}$$

$$\begin{cases} g_i \ge \underline{g}_i u_i \\ g_i + r_i^g \le \overline{g}_i u_i \end{cases} \quad \forall i \in \mathcal{G} \tag{22}$$

$$\begin{cases} u_i = 1 \\ r_i = 0 \end{cases} \quad \forall i \in \mathcal{GS} \tag{23}$$

$$\begin{cases} 0 \le \Delta g_i^q \le r_i^g & \forall i \in \mathcal{GR} \\ 0 \le \Delta d_n^q \le r_n^d & \forall n \in \mathcal{N} \end{cases} \tag{24}$$

Here, (20) imposes a lower bound on the amount of reserves, of either 350 MW (size of the largest generator) or the total amount of SPS tripping capacity. Equation (21) indicates that 4% of load can be committed as demand response. Equation (22) constrain the committed generation and reserve of generator i to lie within $[\underline{g}_i, \overline{g}_i]$, if the generator is committed (u_i), and zero otherwise. Equation (23) ensures that generators in the SPS-connected set $\mathcal{GS}$ are committed and do not participate in reserve services (because they may be disconnected). Equation (24) constrains the activated reserves in the SPS outcome scenario q to lie within the committed range.

Finally, the forced inclusion of generators affected by scenarios in $\mathcal{Q}$ ($\mathcal{S} \in \mathcal{Q}$) is implemented by:

$$t_i = 1 \quad \text{if breaker } i \text{ fails in any } q' \in \mathcal{Q} \tag{25}$$

$$\sum_{i\in\mathcal{GS}_n} t_i \ge 1 \quad \text{if bus } n \text{ comms fail in any } q' \in \mathcal{Q} \tag{26}$$

4.3 Cascading outages and loss of load

The problem (9)–(26) defines candidate solutions $\kappa(\mathcal{Q})$ that are robust to the cyber-physical outcome scenarios in $\mathcal{Q}$. However, the ranking of candidate solutions, requires the explicit evaluation of the risk $X(\kappa)$, necessitating the evaluation of impacts in all scenarios, including non-secure scenarios that may lead to load shedding through a complex cascading pathway. The procedure that is used is described below.

First, the immediate impact of the contingency is evaluated. When the SPS is successfully activated and generator tripping results in an imbalance between generation and demand, the available reserves r_i^g and r_n^d are activated to restore the balance. In many cases—at least for all scenarios in the set $\mathcal{Q}$—there exists an allocation of reserves that avoids residual overloads. However, when this is not possible, they are deployed in such a way that they minimize post-action line overloads according to:

$$\min \sum_{l\in\mathcal{L}} \frac{\max(|f_l| - \overline{f}_l, 0)}{\overline{f}_l} \tag{27}$$

which is reformulated as an MILP model, subject to reserve constraints.

At this point, the system has restored generation balance, but there may be overloads of transmission lines. A quasi steady state cascading algorithm is initiated to explicitly compute the impact of post-SPS scenarios. For this simplified model all generators in a bus are aggregated into a single generator that is characterized by its aggregate output and remaining reserve capacity. It is assumed that the output of this nodal generator can be adjusted to all levels between zero and the sum of the initial output and reserve capacity. The following procedure is repeated until no further overloads are present in the system:

1) All overloaded lines are identified and disconnected simultaneously.
2) Electrical islands are identified.
3) In every island with surplus generation, a proportional reduction in generation output is applied to the generators in the island to balance generation and demand.
4) In every island with a generation deficit, the generator reserve capability is used where possible (proportionally, subject to reserve limits). If the reserve capability is insufficient, load is shed proportionally until the total load equals the maximum generating capacity in the island.
5) DC power flow solutions are computed for the updated generation and load levels.

When no further overloads are found, the aggregate amount of disconnected load (in MW) is multiplied by VoLL and interruption duration to determine the financial impact $L(\mathcal{D}, \mathcal{S}, c, o)$. It is assumed that interruptions last 3 hours.

The model described above is a highly simplified model of cascading that is intended to capture the qualitative behavior of cascades. It can result in very large load losses with a high sensitivity to initial conditions, despite being deterministic, simplifying temporal analysis to a quasi-steady state and relying on simple initiating contingencies $(N-1)$ in combination with simple SPS failures. The methodology presented in this paper could be refined by enhancing the simulation-based evaluation of risks, for example, by taking into account $N-k$, initiating contingencies or stochastic simulations that incorporate additional hidden failures of protection systems [26]. The use of more elaborate simulation methods could only improve the results, because a point-wise comparison of solutions of the type (3) guarantees that the best overall solution is selected, despite simplifications made at the optimization stage.

5 Results

The IEEE RTS case study was implemented in Matlab 2016a, using its interface with FICO Xpress 8.0 to solve mixed-integer linear programming problems. We consider the operation of the system at peak demand (2850 MW) for a period of $\Delta t = 1$ hour. The results are discussed below.

5.1 Optimization of SPS only

As an initial study, we consider a restricted set of decisions where the dispatch $\mathcal{D}$ has been fixed, and the operator only determines the optimal SPS settings $\mathcal{S}$. Because the set of possible SPS settings is finite, it becomes possible to enumerate all SPS configurations and their corresponding outcomes, despite the need to invoke a simulator for each operating point. The objective of this exercise is to illustrate the performance of the greedy steepest descent method by comparing its results to a global optimum obtained by enumeration. For this example, the dispatch is determined through an optimal power flow (OPF) that is secured against the contingencies in set $\mathcal{C}_n$, but not against those in the SPS-triggering contingencies $\mathcal{C}_p$. A minimum reserve requirement of 600 MW is present, in order to enable generation and demand re-balancing after SPS actions.

Table 1 shows the best solutions obtained at each step of the iterative process: the secured scenario sets $\mathcal{Q}_i$, the intertripping generators selected, the total capacity involved (SPS capacity) and the different cost components of each solution. The total cost includes the generation costs $G = \$44369$ associated with the selected dispatch. The risk X is evaluated with respect to the occurrence of contingencies $c \in \mathcal{C}_p$ (because the system has been preventively secured against the others). The bottom row lists the global optimum, and the final column indicates the cost gap between this and the other solutions. In the secured scenario sets, $(\mathcal{C}_p, o_{ok})$ denotes set of scenarios in which the SPS works as expected. It is followed by a specific set of

Table 1 Iterative partial security scenario search, with fixed dispatch

Round	Solution	Secured scenario set ($\mathcal{Q}$)	SPS configuration	SPS capacity (MW)	P (\$)	X (\$)	Total (\$)	Gap (\$)
0	κ_0	$\{(\mathcal{C}_p, o_{ok})\}$	$t_5, t_6, t_7, t_8, t_9, t_{10}$	300	18390	13130	75499	9298
1	κ_1	$\{(\mathcal{C}_p, o_{ok}), (c_{25\cap 26}, b_{22})\}$	t_2, t_3, t_7	400	18520	4209	67098	896
2	κ_2	$\{(\mathcal{C}_p, o_{ok}), (c_{25\cap 26}, b_{22}), (c_{25\cap 26}, b_{21})\}$	t_2, t_3, t_5, t_7	450	18585	3661	66615	414
3	κ_3	$\{(\mathcal{C}_p, o_{ok}), (c_{25\cap 26}, b_{22}), (c_{25\cap 26}, b_{21}), (c_{25\cap 26}, g_1)\}$	$t_2, t_3, t_5, t_6, t_7, t_8$	550	18715	3117	66201	0
Global optimum			$t_2, t_3, t_5, t_6, t_7, t_8$	550	18715	3117	66201	0

Note: the dispatch cost is \$44369 in all scenarios protected SPS failure scenarios, where g_i signifies the SPS failure mode at the breaker of generator i and b_i represents the failure of the communication link at bus i.

In this example, the method requires three iterations to converge to a minimum cost solution, when no better solutions are found by adding additional SPS failure modes to secure against. In this case, the solution κ_3 is equal to the global optimum found by enumeration of all possible candidates. The method starts with the base case $\kappa_0 = \kappa(\mathcal{Q}_0)$ that has a large optimality gap, largely due to the loss-of-load risk X. The root cause to this high exposure is that all selected generators are located at Bus 22, which increases the risk from a common mode failure at this bus. In the first iteration, the method generates and evaluates a variety of SPS configurations that differ from the base case. The best of these, κ_1, is found by securing the system against the common fault at Bus 22 when the most onerous contingency (lines 25 and 26) occurs. It reduces the risk X by diversifying the SPS capacity among Buses 18, 21 and 22, and by committing an additional 100 MW of SPS capacity. The next two iterations provide further robustness to the SPS in case of the double line contingency event, securing the system against the common failure to trip generation in Bus 21 and a failure to trip generator 1 in Bus 18. This is achieved by committing an extra 100 MW of generation in Bus 22.

5.2 Co-optimization of dispatch and protection

We proceed to the extended problem of co-optimizing generator dispatch and SPS settings. In this case, the space of possible solutions is no longer restricted to a finite set of scenarios, as the generator outputs do not correspond to discrete variables. Hence, in contrast with the previous section, we can no longer compare the candidate solutions to a global optimum obtained by enumeration.

Table 2 shows the properties of the solutions obtained. The control of the dispatch constitutes many new degrees of freedom for the optimization and the method has more options to find new solutions in each iteration. In particular, the optimizer can decide on the output of generators and the provision of reserves. The generation SPS column indicates the total allocated SPS capacity. The generation curtailment column indicates the reduction in generation output in the exporting area (north), compared to the case where security considerations are ignored for $c \in \mathcal{C}_p$. For this case, we explicitly show the diverse properties of candidates evaluated in each round. For brevity, only three candidates $\tilde{\kappa}_i^j$ per iteration are shown, including those with the lowest cost (κ_i, highlighted in bold type). The method takes three iterations to converge to the final candidate.

In general, we observe how the allocation of costs to dispatch, protection and risks varies strongly between candidate solutions. This diversity is shown in the first iteration. For example, the candidate $\tilde{\kappa}_1^3$ proposes to commit extra SPS capacity and slight generation curtailments. It also diversifies the SPS capacity among Buses 18, 21 and 22. The end result is a significant reduction of the expected loss-of-load costs at the expense of higher dispatch and protection costs. On the other hand, $\tilde{\kappa}_1^2$ proposes the same SPS configuration and has the same dispatch costs as the base case. However, it achieved better results through an allocation of reserves that happens to ease the impact of non-secured scenarios. The method was able to evaluate such second-order benefits by evaluating the true cost of each candidate.

In the second iteration, a new set of candidate solutions is derived from the best round-1 solution $\kappa_1 = \tilde{\kappa}_1^2$. The best candidate, $\kappa_2 = \tilde{\kappa}_2^3$, eliminates the risk from a complete failure to trip generators at Bus 22 in response to a fault in transformer 7 or a double circuit failure at lines 25 and 26. This is achieved through a combination of generation curtailments and extra SPS capacity; it opts for committing SPS capacity at Bus 21 (g_4) to diversify the SPS response. The other two candidates shown heavily rely on an increase in generation curtailments and protection costs in order to minimize the risk exposure—yet not enough gain is achieved to compensate these extra costs.

The third iteration improves the overall cost by enhancing the security profile associated with communication failures to Bus 21. In particular, the selected candidate secures against this event when a contingency in line 7 triggers the SPS. Interestingly, this is exclusively achieved by improving the deployment pattern of reserves, thus no extra generation and protection costs are required. This example illustrates the importance of the spatial allocation of reserves in highly-congested networks. The algorithm finishes after the third iteration as no further improvements are achieved by adding another scenario to the secured set.

We compare the solution κ_3 found using the proposed steepest descent procedure against five alternative solutions shown in the bottom rows of Table 2. The first is the unconstrained dispatch, which features the lowest generation and protection costs, but naturally carries the highest risk. A second point of comparison it the dependability assumption (κ_0), which still carries higher risks. The final three solutions take into account the fallibility of the SPS to varying extents. The G-1 solution secures the system against non-responsiveness of any single generator. This is achieved by adding all relevant contingency-failure mode combinations to the secured set, and omitting the constraint (25) (because every solution is affected by faults). The B-1

Table 2 Iterative partial security scenario search (with variable dispatch) and alternative solutions (for comparison)

Round	Solutions	Secured scenario set $[\mathcal{Q}]$	SPS config	Gen. SPS (MW)	Gen. curt. (MW)	G (\$)	P (\$)	X (\$)	Total (\$)
Base case	$\boldsymbol{\kappa}_0$	$\{(\boldsymbol{\mathcal{C}_p}, \boldsymbol{o_{ok}})\}$	$\boldsymbol{t_5}, \mathbf{t_6}, \mathbf{t_7}, \boldsymbol{t_8}, \boldsymbol{t_9}, \boldsymbol{t_{10}}$	**300**	**0**	**42959**	**10890**	**1535**	**55384**
1	$\tilde{\kappa}_1^1$	$\{(\mathcal{C}_p, o_{ok}), (c_7, g_1)\}$	t_1, t_5, t_7, t_8	310	0	42959	10903	2311	56174
	$\tilde{\boldsymbol{\kappa}}_1^2 = \boldsymbol{\kappa}_1$	$\{(\boldsymbol{\mathcal{C}_p}, \boldsymbol{o_{ok}}), (\boldsymbol{c_7}, \boldsymbol{b_{22}})\}$	$\boldsymbol{t_5}, \boldsymbol{t_6}, \boldsymbol{t_7}, \boldsymbol{t_8}, \boldsymbol{t_9}, \boldsymbol{t_{10}}$	**300**	**0**	**42959**	**10890**	**1483**	**55332**
	$\tilde{\kappa}_1^3$	$\{(\mathcal{C}_p, o_{ok}), (c_{25\cap26}, b_{21})\}$	t_2, t_3, t_5	398	2	43060	12457	1294	56811
	$\tilde{\kappa}_1^{i>3}$	$\ldots$							
2	$\tilde{\kappa}_2^1$	$\{(\mathcal{C}_p, o_{ok}), (c_7, b_{22}), (c_{25\cap26}, g_1)\}$	$t_1, t_5, t_6, t_8, t_9, t_{10}$	368	42	45074	11518	1198	57790
	$\tilde{\kappa}_2^2$	$\{(\mathcal{C}_p, o_{ok}), (c_7, b_{22}), (c_{25\cap26}, g_4)\}$	t_4, t_5, t_6, t_7, t_8	398	92	47599	12457	1188	61244
	$\tilde{\boldsymbol{\kappa}}_2^3 = \boldsymbol{\kappa}_2$	$\{(\boldsymbol{\mathcal{C}_p}, \boldsymbol{o_{ok}}),(\boldsymbol{c_7}, \boldsymbol{b_{22}}), (\boldsymbol{c_{25\cap26}}, \boldsymbol{b_{22}})\}$	$\boldsymbol{t_4}, \boldsymbol{t_5}$	**338**	**2**	**43060**	**10939**	**1314**	**55313**
	$\tilde{\kappa}_2^{i>3}$	$\ldots$							
3	$\tilde{\boldsymbol{\kappa}}_3^1 = \boldsymbol{\kappa}_3$	$\{(\boldsymbol{\mathcal{C}_p}, \boldsymbol{o_{ok}}), (\boldsymbol{c_7}, \boldsymbol{b_{22}}), (\boldsymbol{c_{25\cap26}}, \boldsymbol{b_{22}}), (\boldsymbol{c_7}, \boldsymbol{b_{21}})\}$	$\boldsymbol{t_4}, \boldsymbol{t_5}$	**338**	**2**	**43060**	**10939**	**1293**	**55292**
	$\tilde{\kappa}_3^2$	$\{(\mathcal{C}_p, o_{ok}), (c_7, b_{22}), (c_{25\cap26}, b_{22}), (c_{25\cap26}, b_{23})\}$	t_5, t_7, t_9, t_{15}	453	22	44064	14179	2329	60571
	$\tilde{\kappa}_3^3$	$\{(\mathcal{C}_p, o_{ok}), (c_7, b_{22}), (c_{25\cap26}, b_{22}), (c_{27}, b_{18})\}$	t_5, t_7, t_9	298	22	44064	10887	2122	57073
	$\tilde{\kappa}_3^{i>3}$	$\ldots$							

Alternatives	Secured scenario set $(\mathcal{Q})$	SPS config	Gen. SPS (MW)	Gen. curt. (MW)	G (\$)	P (\$)	X (\$)	Total (\$)
Unconstrained	$\emptyset$	n/a	n/a	0	42959	10500	9303	62762
Dependable (κ_0)	$\{(\mathcal{C}_p, o_{ok})\}$	$t_5, t_6, t_7, t_8, t_9, t_{10}$	300	0	42959	10890	1535	55384
G-1	$\{(\mathcal{C}_p, o_{ok}), (\mathcal{C}_p, \text{anygen})\}$	$t_3, t_5, t_6, t_7, t_8, t_9, t_{10}$	410	0	42959	12833	1199	56992
B-1	$\{(\mathcal{C}_p, o_{ok}), (\mathcal{C}_p, \text{anyelement})\}$	t_1, t_3, t_5, t_6, t_7	366	54	45680	11456	637	57773
Preventive	all failure scenarios	not used	0	292	61644	10500	0	72144

solution secures the system against communication faults that simultaneously affect all generators at a bus. The constraint (26) was omitted to obtain this solution. Both solutions achieve higher security levels than κ_3, but this is outweighed by significantly higher expenditure on protection and, in case of B-1, generation. A final point of reference is the preventive dispatch solution that corresponds to hedging against a complete failure of the SPS. Although risks are fully mitigated in this case, the operation costs are much higher overall. Compared to the other solutions, κ_3 presents an appealing balance between generation, protection and loss-of-load costs.

Even though it outperforms the listed alternatives, the (global) optimality of the partial security solution κ_3 cannot be ascertained. However, a very conservative lower bound to the total cost of such a solution can be established as follows. The unconstrained dispatch does not secure the system against SPS-connected contingencies $\mathcal{C}_p$ and therefore achieves the lowest possible generation and protection costs, which will bound from below those costs components of the optimal solution. Hypothetically, the optimal solution could eliminate risks altogether ($X = 0$), so that a lower bound is obtained as $G|_{\kappa_0} + P|_{\kappa_0} = \$53459$. With a total cost of \$55292, the partial security solution κ_3 is significantly closer to this conservative lower bound than most alternatives, as well as offering a slight improvement on the dependability assumption (κ_0).

Table 3 Comparison of solutions for the two area network, for different levels of communication dependability *R*

R	Solution	*G* ($)	*P* ($)	*X* ($)	Total ($)
0.9	Partial	131059	13091	12042	156193
	Unconst	127588	10500	577309	715397
	Depend	130513	13091	19289	162894
	G-1	134216	12721	12170	159107
	B-1	**135107**	**13091**	**5944**	**154142**
	Prevent	143934	10500	0	154434
0.95	**Partial**	**131059**	**13235**	**8181**	**152475**
	Unconst	127588	10500	577309	715397
	Depend	130513	13235	12218	155966
	G-1	134216	12845	8150	155210
	B-1	135107	13235	4368	152710
	Prevent	143934	10500	0	154434
0.99	**Partial**	**131059**	**13351**	**5094**	**149504**
	Unconst	127588	10500	577309	715397
	Depend	130513	13351	6288	150152
	G-1	134216	12943	4934	152093
	B-1	135107	13351	3806	152263
	Prevent	143934	10500	0	154434

Note: Solution labels are: partial (iterative partial security); unconst (unconstrained); G-1 (robust against single generator failure); B-1 (single communication link failure); prevent (full preventive security). Lowest cost solutions are indicated in bold type

5.3 Two-area system

We finally present an application on a larger power system, which will be used to illustrate the behaviour of solutions as a function of SPS dependability and the scalability and performance of the method. The power system under consideration is based on the two-area IEEE RTS system: the RTS system presented in the previous section (area A) is linked through three tie-lines to an identical system (area B) [24]. An incentive to make an economic use of the network is created by assuming that the generation in area B is 50% more expensive than that in area A. An extra unit is connected in node 18 (area A) with a maximum and minimum generation capacity of 200 MW and 100 MW, with no associated generation cost. The generation rejection scheme is connected to the same units of area A as in previous sections. However, the dominant power flows from area A to area B lead to further transmission constraints. To alleviate these conditions, we extend the set of line contingencies that trigger an SPS response to include single faults on lines 7, 23, 25, 26, 27, 28, 29 as well as to double circuit faults in lines 25 and 26, all in area A (see Fig. 2). The fault rates of additional lines linked to the SPS are taken equal to that of λ_{27}.

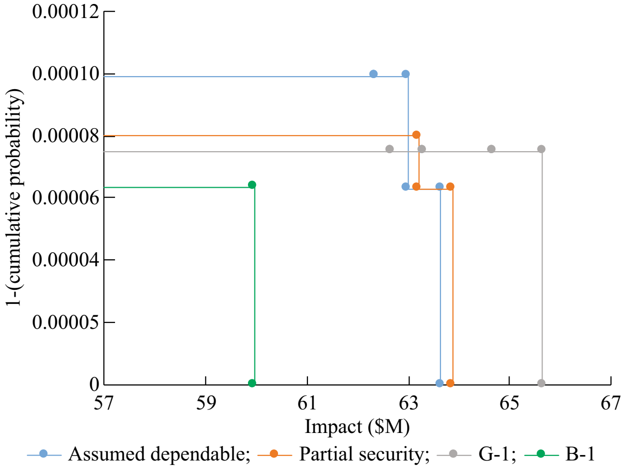

Fig. 4 Risk exposure of solutions visualised by the complementary cumulative probability distribution of loss of load costs

Table 3 shows the results obtained with the proposed iterative partial security method, compared to the alternative approaches discussed above. The different cost components for each solution are analysed for three different SPS dependability scenarios. These are obtained by assigning the dependability of the controller-to-bus communication in (the 'bus' elements in Fig. 3) a value of 0.9, 0.95 and 0.99, respectively.

As was the case in the single area system, the alternative solutions represent a sequence of decreasing loss-of-load risk (*X*), with the proposed partial security solutions providing a risk level in between the assumed-dependable solution and the G-1 solution. For moderate and high reliability of the communication systems (0.95 and 0.99), the partial security solution has the lowest overall cost, reiterating the benefit from partially securing the system against protection faults. It is only for the lowest communication reliability that the B-1 solution provides a better solution, by reducing the risk at the expense of increasing both the generation and protection components.

Figure 4 takes a closer look at the differences in risk exposure between solutions. It shows the complementary cumulative distribution function of loss of load costs, i.e. the probability that certain cost levels are exceeded. Curves are shown for the $R = 0.99$ case, and the dependable, partial security, G-1 and B-1 solutions. The preventive solution is not shown because the is no associated loss-of-load risk, and the unconstrained solution is not listed due to excessive loss of load risk (outside the figure). This representation shows that the loss-of-load risks of the B-1 solution are due to events that are both smaller in impact and less likely than those for other solutions. The partial security solution involves risks that are most similar to the G-1 solution: slightly smaller in terms of impact but more likely to be triggered.

Table 4 Performance metrics for solutions on the single area and two area networks

Performance	One area	Two areas
SPS-triggering contingencies	3	8
Unique SPS failure modes	11	11
Number of iterations to converge	3	2
Candidates evaluated	133	265
Total time (s)	718	5013
Average time per candidate (s)	5.4	18.9
Average time for candidate generation (s)	1.4	7.2
Average time for risk evaluation (s)	3.9	11.7

Table 4 summarises the computational performance of the method, running on an Intel Xeon E5-2690 CPU (8 cores, 2.90 GHz). The number of candidates evaluated by the partial security method is $[1 + (J + 1) \times |\mathcal{C}_p| \times |\mathcal{O}|]$, where J is the number of iterations until the lowest-cost candidate is found and $\mathcal{O}$ is the number of unique failure modes. The two area system used in the example had a greater number of SPS-triggering contingencies, but required fewer iterations to converge, resulting in the evaluation of fewer candidates. However, the larger system size roughly doubles the number of variables in the optimisation problems used for OPF and post-SPS redispatch and cascading failure simulation, leading to significantly larger computational requirements for the generation and evaluation of single candidates.

6 Conclusion and future work

This paper has considered the challenge faced by a system operator operating a power system with an automated protection system that is itself subject to failures. The interplay between physical and cyber faults results in potentially complex failure pathways, including cascading failures, that are very difficult to incorporate into an optimal dispatch framework.

We proposed a method to generate approximate solutions to this optimization problem. The method can be considered a generalized SCOPF approach, where the set of secured contingencies is expanded with specific cyber-physical failure modes. However, the selection of these failure modes is not static, but dynamic: an iterative procedure is used to add secured failure modes one at a time. The selection of the failure mode to add in each round is based on point-wise evaluation of the risks. The use of point-wise evaluations is a powerful property that permits embedding of complex impact assessments based on power system dynamics into cost-benefit operational frameworks.

The procedure was developed in detail for a case study of a generation rejection type SPS on the IEEE RTS (single area and two areas). A mixed integer linear programming model was used to generate partial security solutions, and a basic cascading outage model was used to assess impacts of proposed solutions across all cyber-physical outcome scenarios.

For the restricted case of a fixed generation dispatch, we were able to compare the result from the iterative procedure against the global optimum obtained through enumeration. In the case considered, the optimal solution was recovered. In the more general case where the dispatch was co-optimized with the protection settings, a global optimum is not available, but the solution was compared in detail to alternatives, obtained by 1) unconstrained dispatch; 2) assuming perfect SPS operation; requiring robustness against failure to 3a) trip any one generator, 3b) trip all generators on any bus, or 3c) activate the SPS. The solution obtained using the partial security method resulted in a better risk trade-off for the single area system, and the more reliable two-area systems.

The concepts and method presented in this paper are equally applicable to protection systems that are more complex than the one studied in Sections 4 and 5. More advanced applications include the coordination of multiple SPSs, or SPSs that differentiate responses according the initiating contingency, or more realistic models of power system dynamics. Moreover, although this paper has considered only faults that originated in the physical domain, the same approach can also be applied to cases where faults originate in the cyber domain (e.g. accidental activation of a response).

The method currently relies on a greedy algorithm to search the space of partial security candidates: one secured failure mode is added at a time until no further improvement is found. Of course, despite the good results obtained above, these are likely to be local optima, and pursuing a more advanced search strategy may be worthwhile. As a simple extension, all combinations of k failure modes could be tried, or one could use a stochastic metaheuristic such as a genetic algorithm to search the space of partial security candidates.

Finally, it is important to note that the candidate selection procedure is risk-neutral, balancing upfront and loss-of-load costs in expectation. However, depending on requirements, one could reformulate this in a risk-averse manner, weighting the contributions of individual outcome scenarios differently according to the magnitude of their impacts.

Acknowledgements This work was supported by the UK Engineering and Physical Sciences Research Council (EPSRC) (No. EP/K036173/1) (ACCEPT).

References

[1] Khaitan SK, McCalley JD (2013) Cyber physical system approach for design of power grids: a survey. In: Proceedings of 2013 IEEE power and energy society general meeting, Vancouver, Canada, 21–25 July 2013, 5 pp

[2] Singh C, Sprintson A (2010) Reliability assurance of cyber-physical power systems. In: Proceedings of IEEE PES general meeting, Providence, USA, 25–29 July 2010, 6 pp

[3] Lei H, Singh C (2015) Power system reliability evaluation considering cyber-malfunctions in substations. Electr Power Syst Res 129:160–169

[4] Calvo JL, Tindemans SH, Strbac G (2016) Incorporating failures of system protection schemes into power system operation. Sustain Energy Grids Netw 8:98–110

[5] Mccalley J, Oluwaseyi O, Krishnan V et al (2010) System protection schemes: limitations, risks and management. Report, PSERC

[6] Gagnon JM (2007) Defense plans against extreme contingencies. Report, CIGRE

[7] Moreno R, Pudjianto D, Strbac G (2011) Integrated reliability and cost-benefit-based standards for transmission network operation. Proc Inst Mech Eng Part O J Risk Reliab 226(1):75–87

[8] Capitanescu F, Martinez RJL, Panciatici P et al (2011) State-of-the-art, challenges, and future trends in security constrained optimal power flow. Electr Power Syst Res 81(8):1731

[9] Strbac G, Ahmed S, Kirschen D, Allan R (1998) A method for computing the value of corrective security. IEEE Trans Power Syst 13(3):1096–1102

[10] Moreno R, Pudjianto D, Strbac G (2013) Transmission network investment with probabilistic security and corrective control. IEEE Trans Power Syst 28(4):3935–3944

[11] Calvo JL (2015) Balancing benefits and risks of system protection schemes. Dissertation, Imperial College London

[12] Arabzadeh M, Seifi H, Sheikh-El-Eslami MK (2018) A new mechanism for remedial action schemes design in a multi-area power system considering competitive participation of multiple electricity market players. Int J Electr Power Energy Syst 103(3):31–42

[13] Yang JS, Liao CJ, Wang YF et al (2017) Design and deployment of special protection system for Kinmen power system in Taiwan. IEEE Trans Ind Appl 53(5):4176–4185

[14] Choi DH, Lee SH, Kang YC et al (2017) Analysis on special protection scheme of korea electric power system by fully utilizing STATCOM in a generation side. IEEE Trans Power Syst 32(3):1882–1890

[15] Valencia F, Palma-Behnke R, Ortiz-Villalba D et al (2017) Special protection systems: challenges in the chilean market in the face of the massive integration of solar energy. IEEE Trans Power Deliv 32(1):575–584

[16] Panteli M, Crossley PA, Fitch J et al (2014) Quantifying the reliability level of system integrity protection schemes. Transm Distrib 8(4):753–764

[17] Anderson PM, LeReverend BK (1996) Industry experience with special protection schemes. IEEE Trans Power Syst 11(3):1166–1179

[18] McCalley JD, Fu W (1999) Reliability of special protection systems. IEEE Trans Power Syst 14(4):1400–1406

[19] Fu W, Zhao S, McCalley J et al (2002) Risk assessment for special protection systems. IEEE Trans Power Syst 17(1):63–72

[20] Panteli M, Crossley PA (2012) Assessing the risk associated with a high penetration of System Integrity Protection Schemes. In: Proceedings of 3rd IEEE PES innovative smart grid technologies Europe (ISGT Europe), Berlin, Germany, 14–17 October 2012, 7 pp

[21] Zhang Y, Sprintson A, Singh C (2012) An integrative approach to reliability analysis of an IEC 61850 digital substation. In: Proceedings of IEEE power and energy society general meeting, San Diego, USA, 22–26 July 2012, 8 pp

[22] Lei H, Singh C, Sprintson A (2014) Reliability modeling and analysis of IEC 61850 based substation protection systems. IEEE Trans Smart Grid 5(5):2194–2202

[23] Balachandran T, Kapourchali MH, Sephary M et al (2018) Reliability modeling considerations for emerging cyber-physical power systems. In: Proceedings of IEEE international conference on probabilistic methods applied to power systems, Boise, USA, 24–28 June 2018, 7 pp

[24] Grigg C, Wong P, Albrecht P et al (1999) The IEEE reliability test system-1996. A report prepared by the reliability test system task force of the application of probability methods subcommittee. IEEE Trans Power Syst 14(3):1010–1020

[25] Zimmerman RD, Murillo-Sanchez CE, Thomas RJ (2011) MATPOWER: steady-state operations, planning, and analysis tools for power systems research and education. IEEE Trans Power Syst 26(1):12–19

[26] Jia Y, Xu Z, Lai LL et al (2016) Risk-based power system security analysis considering cascading outages. IEEE Trans Ind Inf 12(2):872–882

Jose Luis CALVO received the Ph.D. degree in 2015 from Imperial College London, UK. He is now with National Grid UK. His research interests include power system reliability assessments and smart grid applications.

Simon H. TINDEMANS received the Ph.D. degree from Wageningen University, The Netherlands, in 2009. He was previously with Imperial College London, UK. He is now an Assistant Professor in the Intelligent Electrical Power Grids section of the Faculty of Electrical Engineering, Mathematics and Computer Science at Delft University of Technology. His research interests include statistical analysis, predictive modelling and control for electrical power systems, combining analytical modelling and stochastic simulation.

Goran STRBAC is a Professor of Electrical Energy Systems with Imperial College London. His research interests include modelling and optimization of electricity system operation and investment, economic and pricing, and integration of new forms of generation and demand technologies.