Fast Generation Redispatch Techniques for Automated Remedial Action Schemes

Hao Huang[§], Maryam Kazerooni [*], Shamina Hossain-McKenzie[†], Sriharsha Etigowni[‡], Saman Zonouz[‡], and Katherine Davis[§]

[§]*Texas A&M University*, *College Station, Texas, USA*, {hao_huang, katedavis}@tamu.edu

[*]*Citadel LLC, New York City, USA* kazerooni.maryam@gmail.com

[†]*Sandia National Laboratories,Albuquerque, New Mexico, USA* shossai@sandia.gov

[‡]*Rutgers University, Piscataway, New Jersey, USA* {se260, saman.zonouz}@rutgers.edu

***Abstract*—To ensure power system operational security, it not only requires security incident detection, but also automated intrusion response and recovery mechanisms to tolerate failures and maintain the system's functionalities. In this paper, we present a design procedure for remedial action schemes (RAS) that improves the power systems resiliency against accidental failures or malicious endeavors such as cyber attacks. A *resilience-oriented optimal power flow* is proposed, which optimizes the system security instead of the generation cost. To improve its speed for online application, a fast greedy algorithm is presented to narrow the search space. The proposed techniques are computationally efficient and are suitable for online RAS applications in large-scale power systems. To demonstrate the effectiveness of the proposed methods, there are two case studies with IEEE 24-bus and IEEE 118-bus systems.**

***Index Terms*—Contingency analysis, generation redispatch, optimal power flow, power system resiliency, remedial action scheme.**

I. Introduction

A power system is a cyber-physical critical infrastructure system that integrates cyber network with physical infrastructure to meet society's electricity needs. While increased connectivity and communications can improve stability, reliability, and efficiency, they also introduce cyber-enabled physical disruptions. Vulnerability of power systems to cyber attacks has increased over the past years due to the growing use of communication technologies and the increasing diversity of the system components. Cyber-physical attacks compromise multiple components in the system in a coordinated fashion, making the traditional operating procedures unsuitable for those contingencies. StuxNet [1], [2], to CrashOverride in Ukraine [3], [4], to new threats reported almost daily have raised awareness of the deeper problem, and call for a holistic solution [5].

Remedial action schemes (RAS) also known as special protection schemes (SPS) are the effective solution to the growing concerns on cyber-physical security [6]–[8]. RAS is an automatic protection system designed to detect abnormal or predetermined system conditions with corrective actions to restore the power system's safe operational mode [9], [10]. The economic and security benefit offered by RAS has urged many utilities to implement them in their systems [11]. RAS are widely deployed by Southern California Edison [12], Bonneville Power Administration (BPA) [13] and British Columbia transmission corporations (BCTC) [14]. Existing RAS designs can be classified based on their type of control action, e.g., generation redispatch [15]–[17], generation tripping [18], [19], load shedding [20], [21] and line switching [22]–[25].

978-1-7281-3192-4/19/$31.00 c 2019 IEEE

Conventional remedial action schemes (RAS) are unsuitable for cyber attacks. Cyber attacks may exhibit dynamic, unpredictable trajectories that cannot be planned against before it occurs. Advanced persistent threats (APTs) [26] require dynamic control selection and response to combat an increasingly complex adversary to achieve more sophisticated goals, and the purpose of this work is to provide the mechanism for such a control solution to be achieved in a fast manner. This paper addresses the question of what to do next: *if the cyber-physical state reveals a cyber attack, how do we quickly respond?*

In this paper, we propose an automated RAS procedure to protect large-scale power systems against accidental failures or malicious endeavors such as cyber attacks with focus on generation redispatch. Two generation redispatch algorithms are proposed: A) *resilience-oriented optimal power flow* that optimizes the system security instead of the generation cost, B) a heuristic-based fast greedy algorithm through control subspace synthesis to narrow the search space. The computation complexity of the proposed algorithms are analyzed and relaxations are employed to improve the running time for online RAS applications in large-scale power systems. The performance of the proposed design procedures is evaluated through simulation using the small IEEE 24-bus and the medium-size 118-bus system.

The contributions of this paper are as follows:

- A security oriented optimal power flow (OPF) is formulated and a resilience-oriented generation redispatch is developed.
- We proposed a greedy algorithm to calculate the optimal generation redispatch using control subspace synthesis. Proper heuristics are considered to narrow down the search space without compromising the performance.
- A security assessment measure considering system constraints is proposed to evaluate the security of each candidate action and is used to select secure candidates.
- An algorithm to identify the critical generators that should participate in RAS is also developed to reduce the computation complexity.

The paper is organized as follows: The resilience-based optimal power flow analysis is presented in Section II. Section III introduces the security-compliant control subspace synthesis and relaxations for the proposed resilience-oriented optimal power flow. Section IV demonstrates the case studies of proposed design procedure using IEEE 24-bus and IEEE 118-bus systems. In Section V, it presents the conclusion and discusses the future work.

Accepted for publication in IEEE 20th International Conference on Intelligent Systems Applications to Power Systems (ISAP), December 2019

II. Resilience -oriented Optimal Power Flow

We present an automated procedure to design RAS with the *resilience-oriented optimal power flow*. The generated RAS logic attempts to keep the power system secure against the potential contingencies. Contingency analysis is first performed to identify all incidents that make the power system insecure, such as overflow, under voltage, etc. A remedial action is then calculated that brings the system back to its normal safe state. The automated RAS design is developed with respect to optimal power flow below.

A. Optimal Power Flow (OPF) Overview

The following equations give a brief overview of optimal power flow (OPF) [27]–[30]. OPF minimizes the operation cost and satisfies the power flow equations and other physical constraints:

$$\begin{aligned} &min\ f(x, u) \\ &s.t.\quad g(x, u) = 0 \\ &\qquad h(x, u) \le 0 \end{aligned} \tag{1}$$

where u is the control variable and x is the state variable. The control variables are the generator real power output set-points, static VAR compensators, settings of the flexible alternating current transmission system (FACTS) devices, phase shifting transformers, etc. The state variables include each bus's voltage magnitude and phase angle. In [31], PV buses' voltage magnitude and slack bus's voltage magnitude and angle are known to solve power flow. To generalize the objective function, only the generator real power output is considered as control variable and the objective function is written as:

$$min \sum_{i \in U_{PV}} C_i(P_i) \tag{2}$$

where $C_i(P_i)$ is the cost of operating generator i with the real power output of P_i, and U_{PV} is the set of PV buses (generators). The voltage magnitudes and phase angles are state variables (x) and can be calculated for a given set of generator real power outputs through solving power flow.

The equality constraint $g(x, u)$ corresponds to the power flow equations and ensures the balance of active and reactive power at the load buses (PQ buses) and generator buses (PV buses and slack bus). The inequality constraint $h(x, u)$ may include the line flow limits, the voltage magnitude limits and the generators output limit as given by:

$$\begin{aligned} &\underline{V}_i \le V_i \le \bar{V}_i \quad i \in U_{PQ} \\ &\underline{P}_i \le P_i \le \bar{P}_i \quad i \in U_{PV} \\ &\underline{Q}_i \le Q_i \le \bar{Q}_i \quad i \in U_{PV} \\ &-\bar{P}_{ij} \le P_{ij} \le \bar{P}_{ij} \quad (i, j) \in I \end{aligned} \tag{3}$$

where V_i, P_i and Q_i are respectively the voltage magnitude, the active power and the reactive power at bus i; and U_{PQ} is the set of PQ buses. We use the notations $\underline{x}$ and $\bar{x}$ to indicate the lower and upper limits of variable x throughout the paper. P_{ij} is the active power on the line between buses i and j, $\bar{P}_{ij}$ is the flow limit of this line, and I is the set of all (i, j) for which there is a line connecting bus i to bus j. Note that the generator output limit is a physical constraint and cannot be violated at any time. On the other hand, the voltage and line flow limits are operating constraints that relate to system reliability, and may be formulated as soft constraints. This formulation considers the generation dispatch at one snapshot of time and hence the generators ramping capacity limits are not captured.

B. Resilience-oriented OPF

In the context of security control, the optimal power flow is reformulated as *Resilience-oriented OPF (ROPF)*, which recovers the system from an insecure state to the normal state after a contingency [32].

Conventional OPF minimizes the operation cost subject to the power flow equations and other constraints, which is not suitable during contingencies. As discussed in [33], a sever damaged power network needs to maintain as much load as possible subject to power system operating requirement, including bus voltage limits, branch thermal limits and generator capacity limits. When a contingency occurs, we assume that retaining system security becomes the first priority rather than the operation cost. Hence, the objective function of *ROPF* optimizes the security instead of cost. Generator costs are not included in our *ROPF* formulation, yet it is not necessary to neglect them. As presented in [34], [35], economic factor can be included in security constrained optimal power dispatch under contingencies and it will be future development to incorporate that into the proposed *ROPF*.

Similar to the conventional OPF [27]–[30], *ROPF* also satisfies the power flow equations and physical and operational constraints, including generator output limits, voltage constraints, line flow limits, etc. Unlike the physical constraints, such as generator output capacity, the operational constraints, including the voltage constraints and line flow limits, may be violated and can be formulated as soft constraints since they are operating constraints. These constraints are modeled by the following,

$$V_i^{(c)} \le \bar{\bar{V}}_i + t_i \quad i \in U_{PQ}$$
$$-V_i^{(c)} \le -\underline{\underline{V}}_i + r_i \quad i \in U_{PQ} \tag{4a}$$
$$P_{ij}^{(c)} \le \bar{\bar{P}}_{ij} + s_{ij} \quad (i, j) \in I$$
$$-P_{ij}^{(c)} \le \bar{\bar{P}}_{ij} + q_{ij} \quad (i, j) \in I \tag{4b}$$
$$0 \le t_i, r_i, s_{ij} \tag{4c}$$

where $V_i^{(c)}$ and $P_{ij}^{(c)}$ are respectively the voltage at bus i and line flow at line (i, j) during the contingency c. Similarly, $\bar{\bar{V}}_i$, $\underline{\underline{V}}_i$ and $\bar{\bar{P}}_{ij}$ are the post-contingency voltage and line flow limits as mandated by NERC [10]. Slack variables r_i and t_i are for the voltage upper and lower limits at bus i, respectively. Slack variables s_{ij} and q_{ij} are for upper and lower flow limits of the line between buses i and j, respectively. The slack variables formulate the soft constraints and are penalized in the objective function. The objective function enforces the voltage and line flow limits as expressed in:

$$min\ VV \sum_{i \in U_{PQ}} (2t_i + t_i^2) + (2r_i + r_i^2) + VI \sum_{(i,k) \in I} (2s_{ik} + s_{ik}^2) + (2q_{ik} + q_{ik}^2) \tag{5}$$

where VV and VI are the weigthing parameters chosen with respect to the desired importance of each term.

Note that the *ROPF* formulation is computationally more complex than the regular OPF. The objective function of the regular OPF contains only the control variable (generators dispatch, P_i) whereas the *ROPF* objective function contains the state variables (voltage magnitudes and angles) which adds complexity to the optimization solver. t_i and r_i relate directly to voltage magnitudes as expressed in (4a). s_i depends on the line flow through (4b) which in turn depends on voltage magnitudes and angles through power flow equations. Therefore, the proposed *ROPF* is computationally more expensive to solve than the conventional OPF, which may not be applicable for larger systems. Power system contingencies should be solved as quickly as possible. To ensure the computation speed, the optimization problem is simplified with following relaxations. First, as defined in [36], the equality constraints associated with the power flow equations are linearized, making the optimization problem as *DC-ROPF*. Second, the inequality constraints with voltage limits are removed. The objective function is modified accordingly as follow:

$$min \sum_{(i,j)\in I} (2s_{ij} + s_{ij}^2) + (2q_{ij} + q_{ij}^2) + \sum_{i\in N} u_i \quad (6a)$$

$$s.t: \quad \underline{P}_i \le P_i^{(c)} \le \bar{P}_i \quad i \in U_{PV} \quad (6b)$$

$$\underline{Q}_i \le Q_i^{(c)} \le \bar{Q}_i \quad i \in U_{PV} \quad (6c)$$

$$B_{ij}(\theta_i - \theta_j) = P_{ij}^{(c)} \quad (i,j) \in I \quad (6d)$$

$$\sum_{(i,j)\in I} P_{ij}^{(c)} + P_i^{(c)} - D_i + u_i = 0 \quad i \in N \quad (6e)$$

$$0 \le u_i \le D_i \quad i \in N \quad (6f)$$

$$P_{ij}^{(c)} \le \bar{P}_{ij}^{c} + s_{ij} \quad (i,j) \in I \quad (6g)$$

$$-P_{ij}^{(c)} \le \bar{P}_{ij}^{c} + q_{ij} \quad (i,j) \in I \quad (6h)$$

$$0 \le s_{ij} \quad (6i)$$

where D_i is the demand at bus i. Constraint (6e) relaxes the node balance constraint by allowing partial demand fulfillment at each node. In (6f), there is a new variable u_i to allow the imbalance between generation and load, which is bounded by the demand variable at each bus. This unbalance is penalized in the objective function ((6a). In this paper, this simplified *ROPF* with excluding the voltage constraints is termed as *relaxed ROPF*. In the following sections, numerical results show that the *relaxed ROPF* is much faster than the regular *ROPF* but with the same level of effectiveness regarding to contingencies.

III. Security-Compliant Control Subspace Synthesis

The feasible control subspace of the power system with n generators is discretized into equally distant n-dimensional cubes. Each generator's MW range is partitioned by equally spaced points. Consequently, a multi-dimensional mesh grid is constructed to cover all possible combinations of the generator outputs. To improve the efficiency, this section proposes different methods to reduce the searching space and identify the most secure candidates with violation index respectively.

A. Reducing the Search Space

The computation complexity of the control subspace synthesis algorithm is $O(R^n)$, where R is the discretization granularity for all generators; n is the number of participating generators for generation re-dispatch, and $O()$ is the big O time complexity notation. The complexity is exponentially increasing with more participating generators. For a large system with lots of generators, the computation complexity can be burdensome and the optimization problem may be even impossible to solve.

1) Identifying Critical Generators: One approach for reducing the computational complexity is to reduce the number of participating generators. Since individual generators may have different impact on the system security due to their location, capacity, etc., it is possible that some generators cannot help on restoring the system from contingencies. Hence, excluding less significant generators from the whole searching space can reduce the number of candidates meanwhile provide necessary margins to find the solution near optimal. The case studies will demonstrate this idea.

We employ a greedy algorithm to identify the insignificant generators based on graph theory and the proximity measures. For every contingency, violations associate with corresponding lines and buses are identified. The generators close to the areas under stress are classified as crucial and the ones which are further away are labeled as insignificant. A multi-level critical generators identification algorithm is described in Algorithm 1. The most critical generators are determined in the first level of the algorithm and less critical ones are determined in subsequent levels. The levels are executed consecutively until the number of critical generators reaches the threshold.

Algorithm 1 Critical Generator Identification (CGI)

```
1:  procedure CGI(Network State and Limits)
2:      U^1_Critbus = Set of buses with violations
3:      U^1_Critgen = U_PV ∩ U^1_Critbus
4:      k = 1
5:      while Size(U^k_Critgen) < CritgenMax do
6:          U^k_Critbus = U^{k-1}_Critbus ∪ Neighbor(U^{k-1}_Critbus)
7:          U^k_CritGen = U^{k-1}_CritGen ∪ (U_PV ∩ U^k_Critbus)
8:          k = k + 1
9:      end while
10: end procedure
```

In the Algorithm, $U^k_{Critbus}$ and $U^k_{Critbus}$ are respectively the set of critical buses and critical generators at level k. $CritGenMax$ is the user-defined maximum number of critical generators. $Neighbor(x)$ returns the set of first-neighbors for the nodes in set x and $Size(x)$ returns the set size.

2) Filtering Actions based on the System Power Losses: Based on the power losses in the system, we can also exclude some of the non-promising candidates to reduce the computation complexity. For each candidate generation dispatch, the total load is fixed, the real output power of all the generators is known except for the slack bus, which is limited by its capacity. Thus, the mismatch between the total generation and load can be used as a criterion to narrow the search space:

$$\underline{P}_{slack} - \delta \le (P_{Load} - \sum_{i\in U_{PV}} P_i)' P_{slack} \le \bar{P}_{slack} + \delta \quad (7)$$

where P_{Load} is the total load in the system, P_{slack} is the MW output of the slack generator, $\bar{P}_{slack}$ and $\underline{P}_{slack}$ are respectively the upper and lower bounds of the slack generator's MW output and δ is the margin of error. The control subspace synthesis that considers all the possible combinations is referred to as full search and the one with only the critical generators and the system loss filtering is termed as the smart search throughout the paper.

3) Utilizing DCPF: The computation time can be further reduced by using DC power flow (DCPF) to solve the system states for all action candidates. Due to the inaccuracy, the DCPF solution can be used as a fast screening tool to calculate the violation indices for all candidates and choose the top ones. Then, the AC power flow analysis can be only performed on top candidates and choose the best action based on their exact violation indices.

B. Proposed Violation Index

In some scenarios, all possible candidates may not satisfy the security constraints, which requires a specific index to evaluate them and select ones that violate fewer constraints. In this way, they can restore the system to a relatively more secure state. In [37], it introduces a security index, aggregated MVA overload (AMWCO), which evaluates the system security based on the total amount of real power flow overflows:

$$AMWCO^{(c,k)} = \sum_{(i,j)\in I} \max\{0, P_{ij}^{(c,k)} - \bar{P}_{ij}\} \quad (8)$$

where $P_{ij}^{(c,k)}$ is the flow on the line between bus i and j when the contingency c and the action k has been employed. This security index considers only the line overflows, without the consideration of the bus voltage or the generator power limits. Thus, this paper proposes a novel violation index that evaluates the resultant security of the system after an action with the consideration of these constraints:

$$Violation^{(c,k)} = w_I S_I^{(c,k)} + w_V S_V^{(c,k)} + w_P S_P^{(c,k)} + w_Q S_Q^{(c,k)} \quad (9)$$

where $S_I^{(c,k)}$, $S_V^{(c,k)}$, $S_P^{(c,k)}$, and $S_Q^{(c,k)}$ are respectively the security indices of the line flows, bus voltages, generator active power and reactive power for contingency c and action k. w_I, w_V, w_P and w_Q are their corresponding weights that capture varying importance of different violation types. The security index for the line flows is given by

$$S_I^{(c,k)} = \sum_{(i,j)\in I} \frac{\max\{0, P_{ij}^{(c,k)} - \bar{P}_{ij}, \bar{P}_{ij} - P_{ij}^{(c,k)}\}}{\bar{P}_{ij}} \quad (10)$$

which is similar to the aggregate MVA overload in (8) except that the MVA overloads are normalized by the line flow limits.

The violation index for bus voltage and generator limits are defined similarly and normalized by their upper bound limits:

$$S_V^{(c,k)} = \sum_{(i)\in U_{PQ}} \frac{\max\{0, V_i^{(c,k)} - \bar{V}_i, \underline{V}_i - V_i^{(c,k)}\}}{\bar{V}_i} \quad (11)$$

The suggested weights for the violation index are $w_P = w_Q = 100$, $w_V = 1$, and $w_I = 0.3$. Since the physical constraints cannot be violated but the operating constraints may be violated, the weights for the generator limits are much higher than other constraints. The weights for voltage and line flow limits are selected based on a heuristic analysis of PJM transmission planning criteria [38], described as below:

This selection captures the lower sensitivity of the system security to the percentage violation of line flow limits compared to voltage constraints. The pre-contingency and post-contingency MW limits of all the lines in PJM are considered. The percentage difference between the pre- and post-contingency limits are calculated for all the monitored lines through $2|\bar{P}_{ij} - P_{ij}|/(\bar{P}_{ij} + P_{ij})$. The average of these percentage differences is 13% excluding the lines whose post-contingency limits are not available. The average ratio of the pre-contingency to post-contingency limits is 0.83. This excludes the lines whose post-contingency limits are not available and the ones whose pre-contingency and post-contingency limits are the same. Next, the normal and emergency voltage limits used in PJM transmission planning are investigated. These limits depend on the bus KV. For simplicity and without loss of generality, the limits for the 230/345 KV lines are considered. The normal lower limit for a 230/345 line is 0.95 and its emergency limit is 0.92. The percentage difference between the normal and emergency limit is 4%. Note that the average percentage difference between the pre- and post contingency line limits was 13% which is 3.25 times larger than the percentage difference between the normal and emergency voltage limit. This suggests that the system security is less sensitive to the percentage violation of line flow limits compared to voltage constraints. The weights for the line flow and voltage limits are selected accordingly in the violation index; i.e. voltage weight, $w_V = 1$ is 3.25 times larger than line flow weight, $w_I = 0.3$

The importance of using the normalization terms and the weights can be demonstrated through an example. Consider two constraint violations: The first violation is on a bus with voltage magnitude of $V_i = 1.5$p.u and maximum permissible voltage of $\bar{V}_i = 1.05$ p.u. The second violation is on a line with $P_{jk} = 800$ MW, which has a post-contingency MW limit of $\bar{P}_{jk} = 400$ MW. The amount of violation is $(V_i - \bar{V}_i) = 0.45$ and $P_{jk} - \bar{P}_{jk} = 400$ for the second one. The first violation is more severe than the second one, yet its amount is much smaller. With the normalization for each scenario's upper bound limits, the weights are 0.43 for the voltage violation and 1 for the current violation. Considering the weights of $w_V = 1$ and $w_I = 0.3$ it results in 0.43 for the voltage violation and 0.3 for the current violation. Now, the terms corresponding to each constraint that appear in the violation index are normalized and reflect their actual impact to the system security. The current framework is a heuristic approach based on specific planning criteria, which can be extended as a systematic approach.

IV. Case Studies with IEEE 24-B us and IEEE 118-B us Systems

The performance of the proposed algorithm is evaluated through simulation using software written in MATLAB running on a Windows desktop machine. All computation times are given with respect to this environment. Optimized numerical solvers and specialized computing platforms offer

TABLE I
COMPARISON OF THE *ROPF* METHODS FOR THE 24- BUS SYSTEM

Scenario	Number of Violations			Violation Index	Time (sec)
	Gen MW	Voltage	Line Flow		
No Action	0	7	3	0.554	-
ROPF	0	2	0	0.021	338.11
Relaxed ROPF	0	2	0	0.0246	36.87
Relaxed DC-ROPF	0	2	1	0.028	9.1946

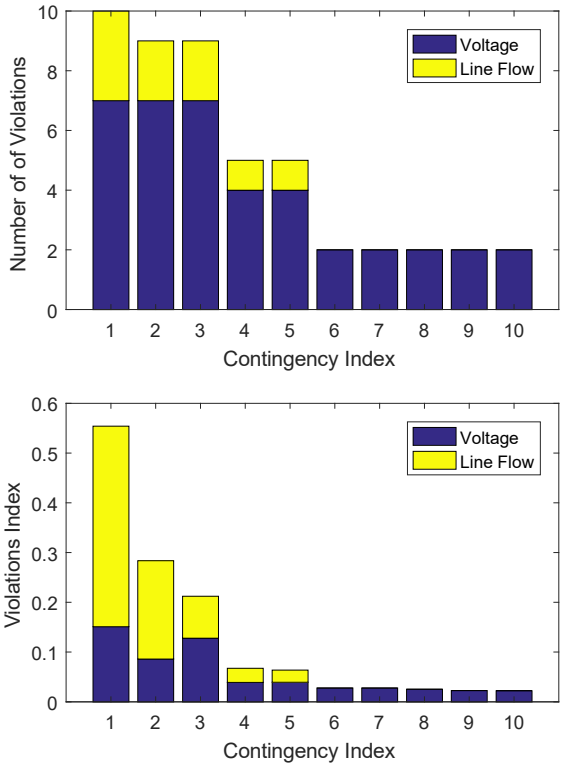

Fig. 1. Contingency analysis of the 24-bus system. The Contingency Index associates with specific single generator outage.

the ability for additional significant improvements; these are outside the scope of the current paper. Optimization of speed across computational environments is a natural next step for a commercial-grade implementation of our solution. In this paper, we perform two case studies on the IEEE 24-bus [39] and the IEEE 118-bus [40] systems to evaluate the proposed algorithms and corresponding relaxation schemes. Contingency analysis is performed, effective RAS actions are designed, and the time consumption of generating RAS based on different relaxation schemes are compared.

1) 24-bus System: First, we perform contingency analysis for single generator outage on the 24-bus system and solve the power flow to calculate the violation index, evaluate the security constraints, and select the most credible contingency. Fig. 1 shows the violation number and violation index broken down by type (voltage and line flow) for all contingencies. It is observed that the number of voltage violations is more than the number of line flow violations. As to the violation index, the generator outage at bus 23 has the highest violation

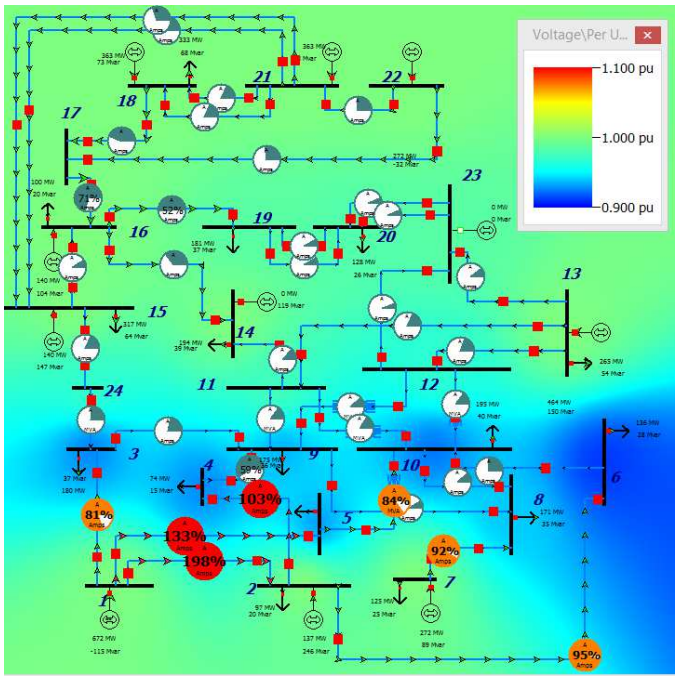

Fig. 2. IEEE 24 Bus case during contingency: The pie charts with red denote the line overflows. The contour plot shows the voltage profile over the system and the blue areas illustrate undervoltage.

index, 0.554, among all the single outages, where the line flow violations contributes more than voltage violations to violation index. This contingency is selected as the most credible one for further analysis. Fig. 2 shows the line flows and the voltage profile of the system after the contingency.

The optimal generation redispatch is obtained through solving *ROPF* under different relaxations and the system security indexes after RAS are presented in Table I. For consistency, the weights of the *ROPF* objective function are selected based on the weights of the violation index, i.e $VV = w_V = 1$ and $VI = w_I = 0.3$. The violation index is reduced from 0.554 to 0.021. However, the computation time for *ROPF* is 338.11 sec, which is too long for a small system. This can be reduced to 36.87 sec by removing the voltage constraints. The *relaxed DC-ROPF* only takes 9.11 sec to obtain the result with a violation index of 0.028, which is much lower than 0.554 and close to the result from ROPF. Since the *DC-ROPF* linearizes the power flow equation with DCPF, the voltage violation under this scenario is calculated by solving ACPF after the generation redispatch is obtained from *DC-ROPF*.

Next, we evaluate the control subspace synthesis for determining the best generation redispatch. The permissible real power output of each generator is divided into four equal intervals, and all possible dispatch scenarios are generated by constructing a multi-dimensional grid based on these intervals. The system has 11 generators, where the generator at bus 1 is the slack generator and the generator at bus 23 is out because of the contingency, so there are 9 generators to construct the control space. The computation complexity is very high according to previous analysis (Section III).

The computation time may be reduced by narrowing down the search space through smart search using proposed filtering techniques. With the CGI algorithm, the critical generators can

TABLE II
CRITICAL GENERATOR IDENTIFICATION (CGI).

CGI Level	Critical Generators
Level 1	2
Level 2	7
Level 3	13,14,15
Insignificant Generators	16,18,21,22

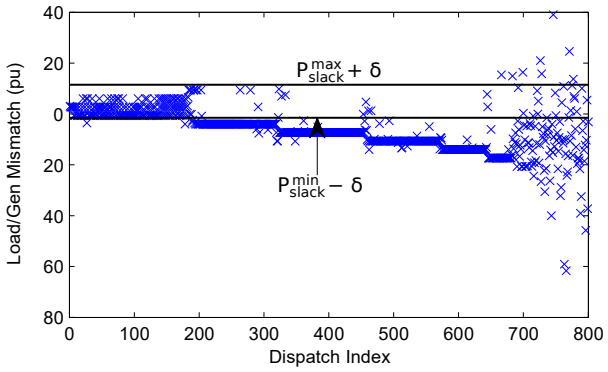

Fig. 3. The mismatch between the total load and generation for the first 800 dispatches when only the critical generators are included in the exhaustive search.

be identified. In this case, the number of critical generator is set to five and the result is shown in Table II. Once the critical generators are determined, the insignificant generators' outputs are fixed to their default values. The smart search is performed on the five critical generators, which reduces the number of combinations and improves the computation speed. With the filtering actions based on the system power loss (Section III), the number of combinations can be further decreased by excluding the non-promising candidates, whose mismatch between total load and generation is too much. With 5 critical generators, there are $4^5 = 1024$ combinations sorted based on their violation index. The mismatch between the total generators real power output (excluding the slack generator) and the total load for the first 800 dispatches is illustrated in Fig. 3. The mismatch falls within the range specified by (7) for the top 27% candidates (first 178 dispatches). Hence, using the load/generation mismatch as a criterion to eliminate non-promising candidates can reduce the number of candidates by an extra 70% without compromising the performance.

The performance of the smart search relies on the correct identification of the critical generators. To demonstrate this, a *Naive Search* that randomly picks the participating generators is considered as opposed to using the proposed CGI algorithm. Table III presents the comparison between different control subspace methods:

(A) *Full Search:* All the possible combinations of generation redispatches are considered.
(B) *Smart Search:* The critical generators are selected and the search is narrowed based on the system losses.
(C) *Naive Search:* Generators are randomly selected to participate in RAS and the search is narrowed based on the system losses.
(D) *Smart search with DCPF:* DCPF is used in the smart search for solving power flow

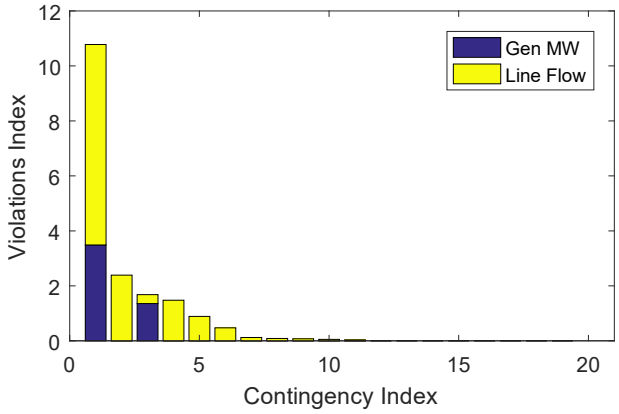

Fig. 4. Contingency analysis for the 118-bus system. The Contingency Index associates with the first 20 largest generators' single outage.

For the full search, it restores the system to a much more secure state than other methods but it takes 10085 sec to determine the RAS scheme, which is impractical for online application. However, the smart search provides the same effectiveness for system security with much less computation time (9.44 sec), which is only 0.09% of the full search running time. The running time from Naïve search is a little longer than smart search and the violation index obtained from the Naïve search is much higher than the smart search, which validates the effectiveness of the CGI algorithm. With DCPF in the smart search, the computation time is much less than smart search but the violation index is not as good as the previous one. This result suggests that, for a smaller system, ACPF can be solved in a satisfied time range with good violation index and it is not necessary to use DCPF to improve the computation sped with less secure control action. Comparing the results of Table I and III, it is observed that *relaxed DC-ROPF* and smart search have equally good performance and efficiency.

2) 118-bus System: Figure 4 illustrates the violation index for single generator outage contingencies for the first 20 largest generators on the IEEE 118-bus system. The contribution of voltage violation is excluded from the figure for better clarity because their values are smaller than 0.001. Line flow violations contribute most for this system's violation index. The generator outage at bus 10 has the highest violation index among all the single outages and is selected for further analysis. Different methods are used to find the best generation redispatch for this contingency. The evaluation of each redispatch method is presented in Table IV. Prior to any actions, the system's violation index is 10.78, consisting of one generator MW violation, three voltage violations and 10 current violations. *Relaxed DC-ROPF* reduces the violation index to only 0.082, yet it takes 1452 sec to solve the problem, which is not practical. Smart search provides almost the same violation index (0.0928) with much lower computation time (282.96 sec). The CGI algorithm is set to find eight critical generators for this system and the control subspace synthesis is constructed with those critical generators that have five intervals. Using DCPF in the smart search reduces the running time by an order of 10 while providing the same violation

TABLE III
COMPARISON OF THE CONTROL SUBSPACE SYNTHESIS METHODS FOR THE 24-BUS SYSTEM

Scenario	Number of Violations			Violation Index	Time (sec)
	Gen MW	Voltage	Line Flow		
No Action	0	7	3	0.554	-
Full Search	0	2	0	0.024	10085
Smart Search	0	2	0	0.024	9.44
Naive Search	0	5-7	1	0.1-0.4	12.8
Smart Search with DCPF	0	6	1	0.128	0.934

TABLE IV
METHOD COMPARISON FOR THE 118-BUS SYSTEM

Scenario	Number of Violations			Violation Index	Time (sec)
	Gen MW	Voltage	Line Flow		
No Action	1	3	10	10.78	-
Relaxed DC-ROPF	0	1	0	0.0825	1452
Smart Search	0	2	1	0.52	282.96
Smart Search with DCPF	0	2	1	0.528	28.59
Naive Search with DCPF	0	3	8-11	5.2-8.8	25.7

index. The Naïve search still takes more time to solve the problem and the violation index from its control action is much higher than the smart search, which also validates the effectiveness of the CGI algorithm and filtering techniques based on load and generation mismatch.

Recall that using DCPF instead of ACPF for the 24-bus system compromises the performance. Meanwhile, the DCPF has better performance on the 118-bus system. The effectiveness of DCPF on the smart search performance depends on the characteristics of the system, such as the transmission network inductance, and the type of post-contingency violations, like overflow or undervoltage. In the 24-bus case, voltage violation dominates the violation index, then the linearization on power flow through DCPF doesn't perform as good as ACPF because the generator real power output doesn't directly impact voltages. However, in the 118-bus case, the overflow violation contributes most for the violation index, the DCPF becomes both effective and efficient, since it captures the coupling between generation redispatch and the line flows.

V. CONCLUSION

This paper presents an automated design procedure for remedial action schemes (RAS) that improves the security of the power system against contingencies. The *resilience-oriented optimal power flow (ROPF)* and *security-compliant control subspace synthesis* are proposed as two generation redispatch techniques that have low computation complexity and are suitable for online RAS applications.

Using the IEEE 24-bus case and the IEEE 118-bus case, we analyze the trade-offs between the security and the computation complexity of the generation redispatch techniques. This allows a system operator to select the best technique to solve the contingency based on the size of the system, the required security measures, etc. The time scale required for these control actions is on the order of seconds to minutes. From the case studies on the IEEE 24-bus case and IEEE 118-bus case, we observe that both methods provide sufficient security for both cases. The running time for the IEEE 24-bus case is fast with both methods, but for the IEEE 118-bus case, the running time of *ROPF* is significantly higher. The greedy algorithm offers a less secure but much faster solution. Comparing different searching algorithms for secure action candidates is also important and will be analyzed in future work.

The paper suggests several opportunities for future research. First, the proposed control subspace synthesis focuses on one particular type of control action, generation redispatch. Future research will extend this framework to focus on real-time cyber attack response using apriori controller priortiziation as in [41]; the proposed online RAS can then dispatch those controls, including both physical and cyber control mechanism. Second, the computation times of the resilience oriented optimal power flow and the critical generators identification may be sped up significantly; the online RAS formulation may be optimized together with state-of-the-art solvers and specialized computing platforms. Third, including economic factors into the proposed *ROPF* is also an important future development for field application.

ACKNOWLEDGMENT

This research is supported by the National Science Foundation (NSF) under Award Numbers 1446471, 1446229 and the US Department of Energy Cybersecurity for Energy Delivery Systems program under award DE-OE0000895.

REFERENCES

[1] C. C. Liu, A. Stefanov, J. Hong, and P. Panciatici, "Intruders in the grid," *IEEE Power and Energy Magazine*, vol. 10, no. 1, pp. 58–66, Jan 2012.

[2] N. Falliere, L. O. Murchu, and E. Chien, "W32.Stuxnet dossier," Symantic Security Response, Tech. Rep., Oct. 2010.

[3] M. J. Assante, "Confirmation of a coordinated attack on the Ukrainian power grid," *SANS Industrial Control Systems*, January 2016. [Online]. Available: ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid

[4] Dragos Security. (2017) Crashoverride: Analysis of the threat to electric grid operations. [Online]. Available: https://dragos.com/blog/crashoverride/CrashOverride-01.pdf

[5] M. Assante. (2011, September) Bad new world: Cyber risk and the future of our nation. [Online]. Available: {http://www.csoonline.com/article/2129606/employee-protection/bad-new-world--cyber-risk-and-the-future-of-our-nation.html}

[6] A. P. Meliopoulos and A. G. Bakirtzis, "Corrective control computations for large power systems," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-102, no. 11, pp. 3598–3604, Nov. 1983.

[7] P. M. Anderson and B. K. LeReverend, "Industry experience with special protection schemes," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1166–1179, Aug. 1996.

[8] C. F. Henville and E. Struyke, "Ras and streched power system," *Western Protective Relaying Conference*, 2006.

[9] T. Liacco, "The adaptive reliability control system," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-86, no. 5, pp. 517–531, May 1967.

[10] "Special protection systems (SPS) / remedial action schemes (RAS): assessment of definition, regional practices, and application of related standards," North American Electric Reliability Corporation (NERC), Tech. Rep., Apr. 2013.

[11] M. Varghese, L. Jin, S. Ghosh, G. Lin, and B. Pek, "The caiso experience of implementing automated remedial action schemes in energy management systems," in *2009 IEEE Power Energy Society General Meeting*, Jul. 2009.

[12] J. Wen, W. H. E. Liu, P. L. Arons, and S. K. Pandey, "Evolution pathway towards wide area monitoring and protection, a real-world implementation of centralized ras system," *IEEE Transactions on Smart Grid*, vol. 5, no. 3, pp. 1506–1513, May 2014.

[13] R. Ramanathan, B. Tuck, and J. O'Brien, "BPA's experience of implementing remedial action schemes in power flow for operation studies," in *2013 IEEE Power Energy Society General Meeting*, Jul. 2013.

[14] S. C. Pai and J. Sun, "BCTCs experience towards a smarter grid - increasing limits and reliability with centralized intelligence remedial action schemes," in *Electric Power Conference, 2008. EPEC 2008. IEEE Canada*, Oct. 2008, pp. 1–7.

[15] I. Genc, R. Diao, V. Vittal, S. Kolluri, and S. Mandal, "Decision tree-based preventive and corrective control applications for dynamic security enhancement in power systems," *IEEE Transactions on Power Systems*, vol. 25, no. 3, pp. 1611–1619, Aug. 2010.

[16] A. A. Fouad, A. Ghafurian, K. Nodehi, and Y. Mansour, "Calculation of generation-shedding requirements of the B.C. hydro system using transient energy functions," *IEEE Power Engineering Review*, vol. PER-6, no. 5, pp. 31–32, May 1986.

[17] D. Ruiz-Vega and M. Pavella, "A comprehensive approach to transient stability control. ii. open loop emergency control," *IEEE Transactions on Power Systems*, vol. 18, no. 4, pp. 1454–1460, Nov. 2003.

[18] H. Ota, Y. Kitayama, H. Ito, N. Fukushima, K. Omata, K. Morita, and Y. Kokai, "Development of transient stability control system (tsc system) based on on-line stability calculation," *IEEE Transactions on Power Systems*, vol. 11, no. 3, pp. 1463–1472, Aug. 1996.

[19] Y. Zhang and K. Tomsovic, "Adaptive remedial action scheme based on transient energy analysis," in *Power Systems Conference and Exposition, 2004. IEEE PES*, Oct. 2004, pp. 925–931 vol.2.

[20] C. W. Taylor, F. R. Nassief, and R. L. Cresap, "Northwest power pool transient stability and load shedding controls for generation-load imbalances," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-100, no. 7, pp. 3486–3495, Jul. 1981.

[21] S. M. Rovnyak, K. Mei, and G. Li, "Fast load shedding for angle stability control," in *Power Engineering Society General Meeting, 2003, IEEE*, Jul. 2003.

[22] W. Shao and V. Vittal, "Corrective switching algorithm for relieving overloads and voltage violations," *IEEE Transactions on Power Systems*, vol. 20, no. 4, pp. 1877–1885, Nov. 2005.

[23] B. Gou and H. Zhang, "Fast real-time corrective control strategy for overload relief in bulk power systems," *IET Generation, Transmission Distribution*, vol. 7, no. 12, pp. 1508–1515, Dec. 2013.

[24] A. A. Mazi, B. F. Wollenberg, and M. H. Hesse, "Corrective control of power system flows by line and bus-bar switching," *IEEE Power Engineering Review*, vol. PER-6, no. 8, pp. 53–53, Aug. 1986.

[25] J. G. Rolim and L. J. B. Machado, "A study of the use of corrective switching in transmission systems," *IEEE Transactions on Power Systems*, vol. 14, no. 1, pp. 336–341, Feb. 1999.

[26] M. K. Daly, "Advanced persistent threat," *Usenix, Nov*, vol. 4, no. 4, pp. 2013–2016, 2009.

[27] H. W. Dommel and W. F. Tinney, "Optimal power flow solutions," *IEEE Transactions on Power Apparatus and Systems*, vol. PAS-87, no. 10, pp. 1866–1876, Oct 1968.

[28] D. I. Sun, B. Ashley, B. Brewer, A. Hughes, and W. F. Tinney, "Optimal power flow by newton approach," *IEEE Transactions on Power Apparatus and systems*, no. 10, pp. 2864–2880, 1984.

[29] A. Monticelli, M. Pereira, and S. Granville, "Security-constrained optimal power flow with post-contingency corrective rescheduling," *IEEE Transactions on Power Systems*, vol. 2, no. 1, pp. 175–180, 1987.

[30] O. Alsac, J. Bright, M. Prais, and B. Stott, "Further developments in lp-based optimal power flow," *Power Systems, IEEE Transactions on*, vol. 5, no. 3, pp. 697–711, Aug 1990.

[31] J. Duncan Glover, M. Sarma, and T. Overbye, *Power System Analysis and Design*, 5th ed. Cengage Learning.

[32] G. Hug-Glanzmann and G. Andersson, "Decentralized optimal power flow control for overlapping areas in power systems," *IEEE Transactions on Power Systems*, vol. 24, no. 1, pp. 327–336, Feb. 2009.

[33] C. Coffrin, R. Bent, B. Tasseff, K. Sundar, and S. Backhaus, "Relaxations of ac maximal load delivery for severe contingency analysis," *IEEE Transactions on Power Systems*, vol. 34, no. 2, pp. 1450–1458, 2018.

[34] J. Zhu, "Security-constrained economic dispatch," 2015.

[35] A. Arab, A. Khodaei, S. K. Khator, and Z. Han, "Electric power grid restoration considering disaster economics," *IEEE Access*, vol. 4, pp. 639–649, 2016.

[36] A. R. Escobedo, E. Moreno-Centeno, and K. W. Hedman, "Topology control for load shed recovery," *IEEE Transactions on Power Systems*, vol. 29, no. 2, pp. 908–916, Mar. 2014.

[37] "D-FACTS devices in PowerWorld simulator." [Online]. Available: http://www.powerworld.com/files/clientconf2014/07Weber_DFACTS.pdf

[38] A. Berner. (2016, aug) Pjm planning criteria-discussion of comparisons for external generation resources. [Online]. Available: https://www.pjm.com/-/media/committees-groups/task-forces/urmstf/20160817/20160817-item-09-pjm-planning-criteria.ashx

[39] P. M. Subcommittee, "Ieee reliability test system," *IEEE Transactions on power apparatus and systems*, no. 6, pp. 2047–2054, 1979.

[40] Synthetic Power Cases-Illinois Center for a Smarter Electric Grid. [Online]. Available: http://icseg.iti.illinois.edu/

[41] S. Hossain-McKenzie, M. Kazerooni, K. Davis, S. Etigowni, and S. Zonouz, "Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment," *IET Cyber-Physical Systems: Theory Applications*, vol. 2, no. 4, pp. 188–197, 2017.