Less is More: Real-time Failure Localization in Power Systems

Linqi Guo, Chen Liang, Alessandro Zocca, Steven H. Low, and Adam Wierman

Abstract— Cascading failures in power systems exhibit non-local propagation patterns which make the analysis and mitigation of failures difficult. In this work, we propose a distributed control framework inspired by the recently proposed concepts of *unified controller* and network *tree-partition* that offers strong guarantees in both the mitigation and localization of cascading failures in power systems. In this framework, the transmission network is partitioned into several control areas which are connected in a tree structure, and the unified controller is adopted by generators or controllable loads for fast timescale disturbance response. After an initial failure, the proposed strategy always prevents successive failures from happening, and regulates the system to the desired steady state where the impact of initial failures are localized as much as possible. For extreme failures that cannot be localized, the proposed framework has a configurable design, that progressively involves and coordinates more control areas for failure mitigation and, as a last resort, imposes minimal load shedding. We compare the proposed control framework with Automatic Generation Control (AGC) on the IEEE 118-bus test system. Simulation results show that our novel framework greatly improves the system robustness in terms of the $N-1$ security standard, and localizes the impact of initial failures in majority of the load profiles that are examined. Moreover, the proposed framework incurs significantly less load loss, if any, compared to AGC, in all of our case studies.

I. INTRODUCTION

Cascading failures in power systems propagate non-locally, making their analysis and mitigation difficult. This fact is illustrated by the sequence of events leading to the 1996 Western US blackout summarized in Fig. 1, in which successive failures happened hundreds of kilometers away from each other (e.g. from stage ③ to stage ④ and from stage ⑦ to stage ⑧). Non-local propagation makes it particularly challenging to design distributed controllers that reliably prevent and mitigate cascades in power systems. In fact, such control is widely considered impossible, even when centralized coordination is available [1], [2].

Current industry practice for mitigating cascading failures mostly relies on simulation-based contingency analysis, which focuses on a small set of most likely initial failures [3]. Moreover, the size of the contingency set which is tested (and thus the level of security guaranteed) is often constrained by computational power, undermining its effectiveness in view of the enormous number of components in power networks. After a blackout event, a detailed study typically leads to a redesign of such contingency sets, potentially together with physical network upgrades and revision of system management policies and regulations [2].

The authors are with the Department of Computing and Mathematical Sciences, California Institute of Technology, Pasadena, CA, 91125, USA. Email: {lguo, cliang2, azocca, slow, adamw}@caltech.edu.
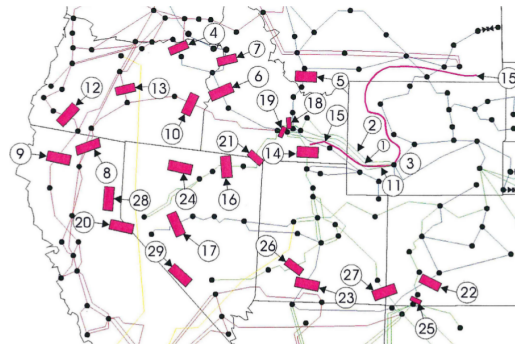
Fig. 1. The sequence of events, indexed by the circled numbers, that lead to the Western US blackout in 1996. Adopted from [17].

The limitations of current practice have motivated a large body of literature to study and characterize analytical properties of cascading failures in power systems. This literature can be roughly categorized as follows: (a) applying Monte-Carlo methods to analytical models that account for the steady state power redistribution using DC [4]–[7] or AC [8]–[10] flow models; (b) studying pure topological models built upon simplifying assumptions on the propagation dynamics (e.g., failures propagate to adjacent lines with high probability) and inferring component failure propagation patterns from graph-theoretic properties [11]–[13]; (c) investigating simplified or statistical cascading failure dynamics [14]–[17]. In all these approaches, the non-local failure propagation often creates significant challenges when trying to make general inferences about failure patterns.

A new approach to address such challenges has emerged in recent years, aiming to improve the system resilience by partitioning the power network into smaller regions and localizing impacts of line failures within each region [18], [19]. This approach is based on the *tree-partition* of power grids (see Section III-A for its definition and properties) and yields many interesting, sometimes counter-intuitive, insights for the planning and management of power systems. For instance, the case studies in [19] show that, by properly reducing system redundancy, one can improve system robustness against component failures – the existence of redundancy turns out to play a prominent role in the non-local nature of failure propagation in power systems.

Unfortunately, this literature has yet to yield a fully satisfactory solution for mitigating and localizing failures, due to two main challenges. First, reducing redundancy as suggested in [18], [19] may lead to single-point vulnerabilities, whose failure has a global impact on the whole system and can potentially cause significant load loss. Second, information on unfolding cascading failures are not fed back into relevant controllers that could adjust the network topology (and in particular its tree-partition). Therefore, after an initial failure is triggered, the strategy described in [19]

guarantees that any successive failure will occur in the same region as the initial failure, but does not prevent or stop successive failures from happening in the first place. To overcome these drawbacks, there is need for new control designs that can "close the loop" and respond actively and promptly to different failures.

Contributions of this paper: *We propose a distributed control strategy that operates on the frequency regulation timescale and offers proveable failure mitigation properties and localization guarantees.* To the best of our knowledge, this control paradigm is the first to leverage results from the frequency regulation literature in the context of cascading failures, bringing new perspectives and insights to both literatures. Our control scheme guarantees that failures do not propagate whenever there is a feasible way to avoid it (see Section III on the rigorous definition of such feasibility), and the impact of failures are localized as much as possible in a manner configurable by the system operator.

We introduce the main idea of our control design in Section IV, whose failure mitigation and localization guarantees are established by the technical results in Section V and VI. The key piece of our control builds upon the so-called Unified Controller (UC), a novel design approach to frequency regulation [?], [20]–[22]. Our design revolves around the new and powerful properties that emerge when the regions that UC manages form a tree-partition. More specifically, in Section V, we characterize how UC responds to an initial failure when it operates over a tree-partition, and prove that a non-critical failure is always mitigated and localized. Later, in Section VI, we discuss how the tree-partition enables the system operator to explicitly specify the unfolding pattern of critical failures, and prove that UC can be extended to detect such scenarios as part of its normal operation.

In order to establish these results, we make use of the correspondence between swing/power flow dynamics and primal-dual algorithms to solve certain optimal dispatch problems, as developed in [20], [22], [23]. Further, we prove new results on the UC optimization problem using novel algebraic characterizations of DC power flow equations derived from graph-theoretic properties of tree-partitions. Lastly, we apply the classical results from convex analysis and optimization theory to show that critical failures can always be detected by UC in a distributed fashion.

In Section VII, we compare the proposed control strategy with classical Automatic Generation Control (AGC) using the IEEE 118-bus test system. We demonstrate that by switching off only a small subset of transmission lines and adopting UC as the fast timescale controller, one can significantly improve the system robustness to failures in terms of the $N-1$ security standard. Moreover, in a majority of the load profiles that are examined, our control strategy further localizes the impact of initial failures to the regions where they occur, leaving the operating points of all other control areas unchanged. Lastly, we highlight that when load shedding is inevitable, the proposed framework incurs significantly less load loss compared to AGC, in all of our case studies.

II. PRELIMINARIES

In this section, we present our power system model, describe the failure propagation process thus derived, and discuss how they are related to previous models in literature.

TABLE I
VARIABLES ASSOCIATED WITH BUSES AND TRANSMISSION LINES.

$\theta := (\theta_j, j \in \mathcal{N})$	bus voltage angle deviations
$\omega := (\omega_j, j \in \mathcal{N})$	bus frequency deviations
$r := (r_j, j \in \mathcal{N})$	injection deviations
$d := (d_j, j \in \mathcal{N})$	mechanical power injection adjustment for generator buses; controllable load adjustment for load buses
$\overline{d}_j, \underline{d}_j, j \in \mathcal{N}$	upper and lower limits for the adjustable injection d_j
$D_j \omega_j, j \in \mathcal{N}$	frequency sensitive generator/load dynamics
$f := (f_e, e \in \mathcal{E})$	branch flow deviations
$\overline{f}_e, \underline{f}_e, e \in \mathcal{E}$	upper and lower limits for branch flow deviations
$C \in \mathbb{R}^{|\mathcal{N}| \times |\mathcal{E}|}$	incidence matrix of $\mathcal{G}$: $C_{je} = 1$ if j is the source of e, $C_{je} = -1$ if j is the destination of e, and $C_{je} = 0$ otherwise
$B := \text{diag}(B_e, e \in \mathcal{E})$	branch flow linearization coefficients that depend on nominal state voltage magnitudes and reference phase angles

A. Power Grid Model and Fast Timescale Dynamics

We consider a power transmission network described by the graph $\mathcal{G} = (\mathcal{N}, \mathcal{E})$, where $\mathcal{N} = \{1, \ldots, |\mathcal{N}|\}$ is the set of buses and $\mathcal{E} \subset \mathcal{N} \times \mathcal{N}$ is the set of transmission lines. The terms bus/node and line/edge will be used interchangeably in the rest of the paper. An edge in $\mathcal{E}$ between nodes i and j is denoted either as e or (i, j). We assign a fixed but arbitrary orientation to the edges in $\mathcal{E}$, so that if $(i, j) \in \mathcal{E}$ then $(j, i) \notin \mathcal{E}$. Together with the variables associated with buses and transmission lines from Table I, the linearized swing and power flow dynamics can be written as

$$M_j \dot{\omega}_j = r_j - d_j - D_j \omega_j - \sum_{e \in \mathcal{E}} C_{je} f_e, \quad j \in \mathcal{N} \quad \text{(1a)}$$

$$\dot{f}_{ij} = B_{ij}(\omega_i - \omega_j), \qquad (i, j) \in \mathcal{E} \quad \text{(1b)}$$

We refer the readers to [20], [22] for more detailed justification and derivation of this model.

Definition 1. *A state $x^* := (\omega^*, d^*, f^*) \in \mathbb{R}^{2|\mathcal{N}|+|\mathcal{E}|}$ is said to be an **equilibrium** of* (1) *if the right hand sides of* (1) *are zero at x^*.*

We emphasize that the d_j's in (1a) usually depend on the system states and may evolve by themselves in accordance to certain controller specific dynamics. The equilibrium defined above refers to the *closed-loop* equilibrium. It is thus possible to engineer the equilibrium of (1) by adopting a different controller design for d_j, which in turn impacts how failures propagate in the system.

B. Failure Occurrence and Propagation

In full generality, the control strategy that we introduce later applies to both generator failures and line failures. However, to simplify the presentation, in this paper we focus only on line failures as the generalization to bus failures is straightforward.[1]

We describe the cascading failure process by keeping track of the set of failed lines at each stage, which are naturally nested and expanding as the stages progress. Overloaded lines are tripped at slower timescales than the dynamics

---

[1]Our results readily apply to cases where the failure of a generator or substation can be emulated by the simultaneous failures of all the transmission lines connected to the corresponding bus.
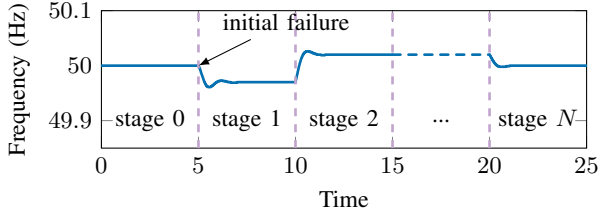
Fig. 2. An illustration of the failure propagation model.

(1); the cascade stages reflect this fact and, indeed, at each stage we *assume* the system reaches the new steady state equilibrium. The crux of our failure propagation model lies in the interplay between such slow timescale line tripping process and the fast timescale dynamics on system transient behavior described by (1), as illustrated in Fig. 2.

More specifically, each stage $n \in \{1, 2, \ldots, N\}$ corresponds to a topology $\mathcal{G}(n) := (\mathcal{N}, \mathcal{E} \backslash \mathcal{B}(n))$ in the failure unfolding process, where $\mathcal{B}(n)$ is the set of all tripped lines at stage n. Within stage n, the system evolves according to the dynamics (1) on the topology $\mathcal{G}(n)$, and converges to an equilibrium point $x^*(n) = (\omega^*(n), d^*(n), f^*(n))$ that depends on $\mathcal{G}(n)$. If all the branch flows $f^*(n)$ are below the corresponding line ratings at equilibrium, then $x^*(n)$ is a secure operating point and the cascade stops. Otherwise, let $\mathcal{F}(n)$ be the subset of lines whose branch flow exceeds the corresponding line ratings. The lines in $\mathcal{F}(n)$ operate above their safety limits in steady state, so by the end of stage n they are overheated and tripped, i.e., $\mathcal{B}(n+1) = \mathcal{B}(n) \cup \mathcal{F}(n)$. Line overloads during the transient phase before the system converges to $x^*(n)$ are considered to be tolerable because the transient dynamics in (1) are not long enough to overheat a line [20] (lasting only seconds to a few minutes). This process repeats for stage $n + 1$ and so on.

C. Recovering Previous Models

Our failure propagation model brings new perspectives to the commonly studied models in literature, and reveals interesting insights on how certain limitations from previous work can be circumvented. In particular, the extra freedom in choosing d_j in the fast timescale dynamics (1) allows us to design and improve how the system reacts to line failures; thus achieving failure mitigation objectives directly using the well-known analytical tools from frequency regulation literature.

As a first example, we show that adopting the classical droop control [24] in our framework recovers cascading failure models from previous literature such as [6], [18], [19], [25]. Indeed, as shown in [20], the closed-loop equilibrium of (1) under droop control is the unique[2] optimal solution to the following optimization:

$$\min_{\omega, d, f, \theta} \quad \sum_{j \in \mathcal{N}} \frac{d_j^2}{2K_j} + \frac{D_j w_j^2}{2} \tag{2a}$$

$$\text{s.t.} \quad r - d - D\omega = Cf \tag{2b}$$

$$f - BC^T \theta = 0 \tag{2c}$$

$$\underline{d}_j \leq d \leq \overline{d}_j, \quad j \in \mathcal{N}, \tag{2d}$$

where K_j's are the generators' participation factors [24]. By plugging (2c) into (2b), it is routine to check that any feasible

---

[2]Such uniqueness is up to a constant shift of all phase angles θ. See [20].

point $x = (\omega, d, f, \theta)$ of (2) satisifes $\sum_j r_j = \sum_j (d_j + D_j \omega_j)$. As a result, the Cauchy-Schwarz inequality implies that

$$\left(\sum_{j \in \mathcal{N}} r_j \right)^2 = \left[\sum_{j \in \mathcal{N}} (d_j + D_j \omega_j) \right]^2$$

$$\leq \sum_{j \in \mathcal{N}} \left(\frac{d_j^2}{2K_j} + \frac{D_j \omega_j^2}{2} \right) \sum_{j \in \mathcal{N}} (2K_j + 2D_j),$$

and equality holds if and only if

$$d_j = \frac{K_j}{\sum_j (K_j + D_j)} \sum_j r_j, \quad \omega_j = \frac{\sum_j r_j}{\sum_j (K_j + D_j)}. \tag{3}$$

Therefore, if the control limits (2d) are not active, (3) is always satisfied at the optimal point $x^* = (\omega^*, d^*, f^*, \theta^*)$.

Now consider a line e being tripped from the transmission network $\mathcal{G}$, and for simplicity assume the control limits (2d) are not active. If e is a bridge[3], the tripping of e results in two islands of $\mathcal{G}$, say $\mathcal{N}_1$ and $\mathcal{N}_2$, and two optimization problems (2) corresponding to $\mathcal{N}_1$ and $\mathcal{N}_2$ respectively. For $l = 1, 2$, $\sum_{j \in \mathcal{N}_l} r_j$ represents the total power imbalance in $\mathcal{N}_l$, and therefore (3) implies that droop control adjusts the system injection so that the power imbalance is distributed to all generators proportional to their participation factors in both $\mathcal{N}_1$ and $\mathcal{N}_2$. If $e = (i, j)$ is not a bridge, denoting the original flow on e before it is tripped as f_e, then $r_i = f_e$, $r_j = -f_e$ and $r_k = 0$ otherwise. As a result, we have $\sum_{j \in \mathcal{N}} r_j = 0$ in this case and thus (3) implies the system operating point remains unchanged. This control recovers exactly the failure propagation dynamics in [6], [18], [19], [25]. Moreover, one can show that this still holds when (2d) is active with a more involved analysis on the KKT conditions of (2).

We thus see that this droop control mechanism underlies some of the previous results in the literature on cascading failures in power systems. In paricular, this suggests that, by using a different control design for d_j, we can obtain different and potentially better system behaviors after a line failure. For instance, it is shown in [19] that bridge failures under droop control have a global impact, while (as we outline in Section V) the impact of bridge failures can in fact be localized using UC. Our new proposed control strategy leverages precisely this extra freedom in chooseing the d_j's to offer stronger guarantees in both failure mitigation and localization compared to previous work [19].

III. Tree-partitions and the Unified Controller

The tree-partition and UC have emerged recently as tools to improve power system robustness [18]–[20]. These concepts have been investigated separately in the literature as they operate at different timescales and aim to solve different problems. Our model brings them together into a novel framework, which allows us to obtain new results combining their strengths and, at the same time, provides new insights for both. In this section, we review these concepts and explain how they come together in this work.

A. The Tree-partition

Given a power system $\mathcal{G} = (\mathcal{N}, \mathcal{E})$, a collection $\mathcal{P} = \{\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_k\}$ of subsets of $\mathcal{N}$ is said to form a *partition*

---

[3]A line e is said to be a *bridge* for $\mathcal{G}$ if it is a cut-edge for $\mathcal{G}$, i.e., if the removal of e from $\mathcal{G}$ disconnects $\mathcal{G}$ into two components, usually referred to as islands in power system literature. See [26] for its rigorous definition.
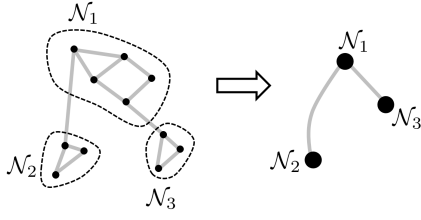
Fig. 3. The construction of $\mathcal{G}_{\mathcal{P}}$ from $\mathcal{P}$.

of $\mathcal{G}$ if $\mathcal{N}_i \cap \mathcal{N}_j = \emptyset$ for $i \neq j$ and $\cup_{i=1}^k \mathcal{N}_i = \mathcal{N}$. For each partition $\mathcal{P} = \{\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_k\}$, we can define a reduced multi-graph $\mathcal{G}_{\mathcal{P}}$ from $\mathcal{G}$ as follows (see Fig. 3). The node set of $\mathcal{G}_{\mathcal{P}}$ is in one-to-one correspondence with $\{\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_k\}$, in the sense that we collapse each subset $\mathcal{N}_i$ into a "super node" of $\mathcal{G}_{\mathcal{P}}$. We then add an undirected edge connecting the super nodes $\mathcal{N}_i$ and $\mathcal{N}_j$ for each pair of nodes $v, w \in \mathcal{N}$ if $v \in \mathcal{N}_i$, $w \in \mathcal{N}_j$ and they are connected in $\mathcal{G}$, i.e. $(v, w) \in \mathcal{E}$ or $(w, v) \in \mathcal{E}$. Note that multiple edges are added when multiple pairs of such v, w exist.

Definition 2. *A partition $\mathcal{P}^{\text{tree}} = \{\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_k\}$ of $\mathcal{G}$ is said to form a **tree-partition** if the reduced multi-graph $\mathcal{G}_{\mathcal{P}^{\text{tree}}}$ is a tree. In this case, the subsets $\mathcal{N}_l$ are referred to as tree-parition **regions** and the edges of $\mathcal{G}$ whose endpoints belong to different regions are called **bridges**.*

It is shown in [19] that each graph $\mathcal{G}$ has a unique irreducible tree-partition, which can be computed in linear time, and for this tree-partition, the concept of bridges defined above coincides with that from classical graph theory literature, such as [26]. The tree-partition of a transmission network encodes rich information about how failures propagate (under droop control, as we discussed in Section II-C).

B. The Unified Controller (UC)

UC is a control approach recently proposed in the frequency regulation literature [**?**], [20]–[22]. Compared to classical droop control or Automatic Generation Control (AGC) [24], UC aims to achieve primary frequency control, secondary frequency control, and congestion management simultaneously at the frequency control timescale.

The key feature of UC that we use here is that the closed-loop equilibrium of (1) under UC solves the following optimization:

$$\min_{f, d, \theta} \quad \sum_{j \in \mathcal{N}} c_j(d_j) \tag{4a}$$

$$\text{s.t.} \quad r - d - Cf = 0 \tag{4b}$$

$$f = BC^T \theta \tag{4c}$$

$$ECf = 0 \tag{4d}$$

$$\underline{f}_e \leq f_e \leq \overline{f}_e, \quad e \in \mathcal{E} \tag{4e}$$

$$\underline{d}_j \leq d_j \leq \overline{d}_j, \quad j \in \mathcal{N}, \tag{4f}$$

where $c_j(\cdot)$'s are associated cost functions that penalize deviations from last optimal dispatch point (and hence attain minimum at 0), (4b) guarantees power balance at each bus, (4c) is the DC power flow equation, (4d) enforces zero area control error [24], (4e) and (4f) are the flow and control limits. The matrix E encodes control area information as follows: Given a partition $\mathcal{P}^{\text{UC}} = \{\mathcal{N}_1, \mathcal{N}_2, \cdots, \mathcal{N}_k\}$ of $\mathcal{G}$ that specifies the control areas in secondary frequency

control, $E \in \{0, 1\}^{|\mathcal{P}^{\text{UC}}| \times |\mathcal{N}|}$ is defined by $E_{l,j} = 1$ if bus j is in region $\mathcal{N}_l$ and $E_{l,j} = 0$ otherwise. An edge $e \in \mathcal{E}$ is called a *tie-line* if its endpoints belong to different regions in $\mathcal{P}^{\text{UC}}$ [20], [24]. As a result, the l-th row of $ECf = 0$ ensures that the branch flow deviations on the tie-lines connected to $\mathcal{N}_l$ sum to zero.

UC is designed so that its controller dynamics combined with the system dynamics (1) form a variant of projected primal-dual algorithms to solve (4). It is shown in [20], [21] that when the optimization problem (4) is feasible, under mild assumptions UC is globally stable and converges to the optimal point of (4). This optimal point is unique (up to a constant shift of θ) if the cost functions $c_j(\cdot)$ are strictly convex. We refer readers to [20], [21] for its exact controller design and analysis.

C. Connecting UC to Tree-partition

In the previous subsections we mention two distinct partitions of a power network: the tree-partition $\mathcal{P}^{\text{tree}}$ and the control area partition $\mathcal{P}^{\text{UC}}$. In general, $\mathcal{P}^{\text{tree}}$ and $\mathcal{P}^{\text{UC}}$ can be different. However, when they do coincide, the underlying power grid inherits analytical properties from both tree-partition and UC, making the system particularly robust against failures. Our proposed control strategy leverages this connection, as we present in more detail in Section IV, and we henceforth assume that $\mathcal{P}^{\text{tree}} = \mathcal{P}^{\text{UC}}$. Under this assumption, the bridges and the tie-lines of the power network $\mathcal{G}$ also coincide.

Definition 3. *Given a cascading failure process described by $\mathcal{B}(n), n \in \{1, 2, \ldots, N\}$, the set $\mathcal{B}(1)$ is said to be its **initial failure**.*

In a power system, it is reasonable to expect that different initial failures can have different levels of impact on the rest of the network. For instance, the disconnection of a single solar panel from the grid is unlikely to cause any disruption to the system operation, while the failure of a transmission line that connects a major generator to the grid may incur significant load shedding. We thus need to distinguish different types of failures and ensure the proposed control scheme reacts accordingly.

Definition 4. *An initial failure $\mathcal{B}(1)$ is said to be **critical** if the UC optimization (4) is infeasible over $\mathcal{G}(1) := (\mathcal{N}, \mathcal{E} \backslash \mathcal{B}(1))$, or **non-critical** if it is not critical.*

To formally state our localization result, we define the following concept to clarify the precise meaning of a region being "local" with respect to an initial failure.

Definition 5. *Given an initial failure $\mathcal{B}(1)$, we say that a tree-partition region $\mathcal{N}_l$ is **associated** with $\mathcal{B}(1)$ if there exists an edge $e = (i, j) \in \mathcal{B}(1)$ such that either $i \in \mathcal{N}_l$ or $j \in \mathcal{N}_l$.*

As we discuss in Section IV, our control strategy provides strong guarantees in mitigation and localization for both non-critical and critical failures, in a way that only the operation of the associated regions are adjusted whenever possible.

IV. PROPOSED CONTROL STRATEGY

Our control strategy revolves around the new and powerful properties of the power system that emerge when the control areas that UC operates over form a tree-partition of the network. In this section, we outline how this strategy can
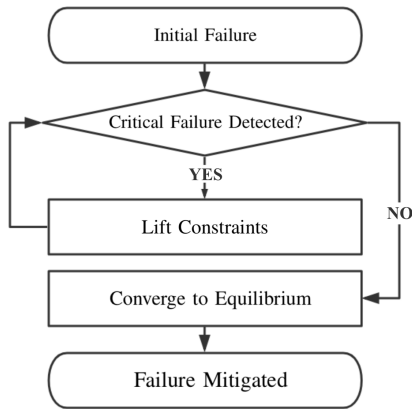
Fig. 4. Flowchart of the events after an initial failure under the proposed control strategy.

be implemented, in both the planning phase, where a tree-partition structure of the control areas should be created, and the operating phase, during which UC actively monitors and reacts to line failures. Fig. 4 illustrates the sequence of events after an initial failure in the proposed control strategy.

A. Planning Phase: Tree-partition of Control Areas

Power networks are often comprised of multiple control areas, each of which is managed by an independent system operator (ISO). Although these areas exchange power with each other as prescribed by economic dispatch, their operations are relatively independent and it is desirable to ensure system disturbances in one area do not have a significant impact on the others. This is usually achieved via the zero area control error constraint in secondary frequency control [24], and is enforced in UC with (4d). As we discuss in Section III-C, such control areas typically do not form a tree-partition of the transmission network, as having redundant lines is believed to be a crucial part in maintaining $N-1$ security of the power system [1], [2], [24].

In order to implement our control strategy, we propose to create a tree-partition whose regions are precisely the control areas over which UC operates. This can be done by switching off a subset of the tie-lines so that the reduced multi-graph obtained from the control area partition forms a tree. The switching actions only need to be carried out in the planning phase as line failures that occur during the operating phase do not affect the tree-partition already in place[4]. It is interesting to note that, when the subset of lines to switch off is chosen carefully, this action not only helps localize the impact of line failures, but can also improve the system reliability in the $N-1$ security sense. This seemingly counter-intuitive phenomenon is illustrated by our case studies in Section VII-A.

B. Operating Phase: Extending the Unified Controller

Once a tree-partition is formed, the power network under UC operates as a closed-loop system and responds to disturbances such as transmission line failure or loss of generator/load in an automonous manner. In normal conditions where the system disturbances are insignificant, UC always

[4]In fact, in certain cases line failures lead to "finer" tree partitions as more regions are potentially created when lines are removed from service.

drives the power network back to an equilibrium point that can be interpreted as an optimal solution of (4). This is the case, for instance, when non-critical failures (see Definition 4) happen and therefore, such failures are always properly mitigated.

However, in extreme scenarios where a major disturbance (e.g. a critical failure) affects the system, the optimization problem (4) that UC aims to solve can be infeasible. In other words, it is physically impossible for UC to achieve all of its control objectives after such a disturbance. This causes UC to be unstable (see Proposition 8) and, further, leads to successive failures or even large scale outages. As such, there is a need to extend the version of UC proposed in [20], [21] with two features: (a) a critical failure detection component that monitors the system states and ensures UC is aware of such extreme situation promptly when it happens; (b) a constraint lifting component that responds to critical failures by proactively relaxing certain goals that UC tries to achieve, and ensures system stability can be reached at minimal cost.

Our technical results in Section VI-A suggest a way to implement both components as part of the normal operation of UC. System operators can prioritize different control areas by specifying the sequence of constraints to lift in response to extreme events. This allows the non-associated regions to be progressively involved and coordinated in a desired pattern when mitigating critical failures. We present and discuss some potential schemes in Section VI-B.

C. Guaranteed Mitigation and Localization

As we show in detail in Sections V and VI, our control strategy provides strong guarantees in mitigation and localization for both non-critical and critical failures. More specifically, the proposed control strategy ensures that, (a) non-critical failures are always fully mitigated by the associated regions, and the operating points for non-associated regions are not impacted at all; (b) critical failures are guaranteed to be mitigated with certain constraints in (4) being lifted, in a progressive manner specified by the system operator. Thus the proposed strategy always prevents successive failures from happening, while localizing the impact of the initial failures as much as possible.

V. LOCALIZING NON-CRITICAL FAILURES

In this section, we consider non-critical failures, as defined in Section III, and prove that such failures are always fully mitigated within the associated regions.

We first characterize how the system operating point shifts in response to such failures. Recall that if an initial failure $\mathcal{B}(1)$ is non-critical, the UC optimization (4) is feasible and thus the new system operating point $x^*(1) := (\omega^*(1), d^*(1), f^*(1), \theta^*(1))^5$ under UC control satisfies all the constraints in (4). In particular, none of the line limits in (4e) is violated at $x^*(1)$, i.e. $x^*(1)$ is a secure operating point and the cascade stops, namely $\mathcal{F}(1) = \emptyset$.

Lemma 6. *Given a non-critical initial failure $\mathcal{B}(1)$, the new operating point $x^*(1)$ prescribed by the UC satisfies $f_e^*(1) = 0$ for every bridge e.*

The above lemma shows that, in addition to the zero area control error constraints enforced by (4d), when the control areas that UC operates over form a tree-partition,

[5]We add θ to the state space of (1) when the phase angle is relevant.

UC further guarantees zero flow deviations on all tie-lines. This demonstrates how a tree-partition enables UC to achieve a stronger performance guarantee compared to its original form as proposed in [20], [21]. The following proposition is another result of this type, which clarifies how the tree-partition brings localization properties to UC.

Proposition 7. *Assume $c_j(\cdot)$ is strictly convex for all $j \in \mathcal{N}$. Given a non-critical initial failure $\mathcal{B}(1)$, if a tree-partition region $\mathcal{N}_l$ is not associated with $\mathcal{B}(1)$, then $d_j^*(1) = 0$ for all $j \in \mathcal{N}_l$.*

This result reveals that, with the proposed control strategy, when the system converges to equilibrium after a non-critical failure, the injections and power flows in the non-associated regions remain unchanged. In other words, our control scheme guarantees that non-critical failures in a control area do not impact the operations of other areas at all, achieving a stronger control area independence than that ensured by the zero control error requirement.

Unlike the scheme in [19], bridge failures in the proposed control strategy are treated in exactly the same way as other lines, provided that they are non-critical. Furthermore, the impact of such bridge failures is localized to the associated regions. This contrast with the global impact of bridge failures in [19] demonstrates again the benefits of connecting UC to tree-partitions.

VI. Controlling Critical Failures

We now consider the case where the initial failure is critical. This may happen when a major generator or transmission line is disconnected from the grid.

A. Unified Controller under Critical Failures

Since UC is a concept that emerged from the frequency regulation literature, the underlying optimization (4) is always assumed to be feasible in existing studies [20], [21]. As such, little is known about the behaviors of UC if this assumption is violated, which is the case when a critical failure happens. We now derive a result that closes this gap and characterizes the limiting behavior of UC in this setting.

In order to do so, we first need to formulate the exact controller dynamics of UC. Unfortunately, there is no standard way to do so as multiple designs of UC have been proposed in the literature [**?**], [20]–[22], each with its own strengths and weaknesses. Nevertheless, all of the proposed controller design are (approximately) projected primal-dual algorithms to solve the underlying optimization (4), and satisfy the following assumptions:

UC1: For all $j \in \mathcal{N}$, $\underline{d}_j \leq d_j(t) \leq \overline{d}_j$ is satisifed for all t. This is achieved either via a projection operator that maps $d_j(t)$ to this interval, or by requiring the cost function $c_j(\cdot)$ to approach infinity near these boundaries.
UC2: Dual variables are introduced for constraints (4b)-(4e) and maintained throughout the operation (denote these dual variables by λ_i for $i \in \left\{ 1, 2, \cdots, |\mathcal{N}| + 3|\mathcal{E}| + |\mathcal{P}^{\mathrm{UC}}| \right\}$).
UC3: The primal variables f, θ and the dual variables λ_i are updated by a primal-dual algorithm[6] to solve (4).

---

[6]We do not consider the specific variants of the standard primal-dual algorithms that are proposed in different designs of UC, since the standard primal-dual algorithm is often a good approximation.

Proposition 8. *Assume UC1-UC3 hold. If* (4) *is infeasible, then there exists a dual variable λ_i such that:*

$$\limsup_{t \to \infty} |\lambda_i(t)| = \infty$$

This result implies that after a critical failure, UC cannot drive the system to a proper and safe operating point. In fact, it always leads to instability in the system (certain dual variables can take arbitrarily large values). This drawback, however, when viewed from a different perspective, suggests a way to detect critical failures. More specifically, since Proposition 8 guarantees certain dual variables will become arbitrarily large in UC operation when (4) is infeasible, we can always set a threshold for the dual variables and raise an infeasibility warning if some of them exceed the corresponding thresholds. By doing so, critical failures can always be detected, and this happens in a distributed fashion in parallel to the normal operation of UC. Moreover, by setting tighter thresholds around the normal operating point, such failures can be detected more promptly.

Of course, this method is subject to false alarms since non-critical failures may also cause relatively large dual variable values in transient state. There is an intrinsic tradeoff on the level of the thresholds to be applied, in the following sense: A tighter threshold allows critical failures to be detected more promptly, yet also leads to a larger false alarm rate. In practice, these thresholds should be chosen carefully by the operator in accordance to the specific system parameters and application scenarios.

B. Constraint Lifting as a Remedy

In the event of a critical failure, it is physically impossible for UC to simultaneously achieve all of its control objectives. Our discussion in the last subsection shows that, if UC still operates following its normal dynamics, the system is subject to instability and thus successive failures. In the worst case, this can lead to large scale outages.

We can prevent this from happening by lifting certain constraints from UC. Without compromising the basic objective to stabilize the system, there are two ways to do so:

- The zero area control error constraints (4d) between certain control areas can be lifted. This in practice means the controller now gets more control areas involved to mitigate the failure.
- Certain load shedding can be applied, which in (4) is reflected by enlarging the range $[\underline{d}_j, \overline{d}_j]$ for the corresponding load buses.

By iteratively lifting the two types of constraints above, one can guarantee the feasibility of (4) and ensure the system under the proposed control converge to a stable point, which in particular is free from successive failures. This, however, comes with the cost of potential load loss, and thus must be carried out properly. In practice, the iterative relaxation procedure can follow predetermined rules specified by the system operator to prioritize different objectives.

VII. Case Studies

In this section, we evaluate the performance of the proposed control strategy on the IEEE 118-bus test system, which comprises of two control areas as shown in Fig. 5. The three dashed lines (15, 33), (19, 34) and (23, 24) are switched off whenever a tree-partition needs to be formed, and the new topology is referred to as the revised network.
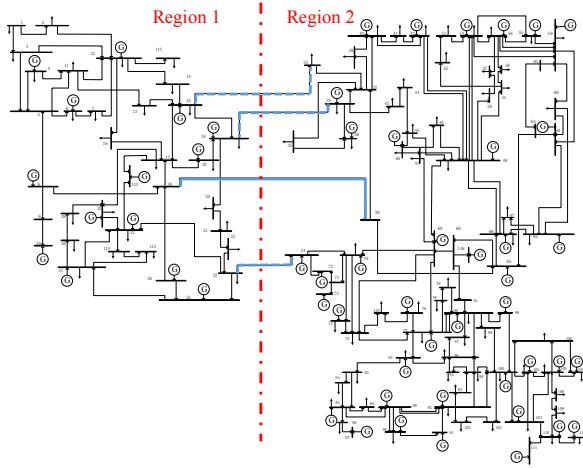
Fig. 5. One line diagram of the IEEE 118-bus test system with two control areas. Dashed blue lines are switched off when a tree-partition needs to be formed.
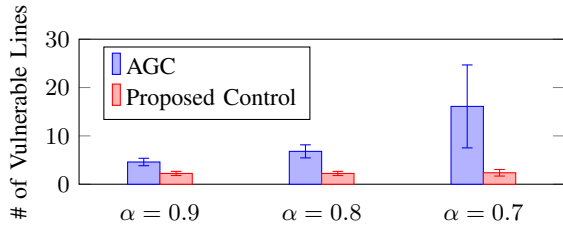

Fig. 6. Number of vulnerable lines with respect to different levels of system congestion.

Fig. 7. CCDF for load loss rate.

Fig. 8. CCDF for generator response.

The failure scenarios to be examined are created as follows. First, we generate 100 load injections by adding random perturbations (up to 25% of the base value) to the nominal load profile from [28] and then solve the DC OPF to obtain the corresponding generator operating points. Second, we iterate over every transmission line in the IEEE 118-bus test system as initial failures and simulate the cascading process thus triggered. This produces about 18,000 scenarios.

A. $N-1$ Security

We first evaluate the system robustness to failures in terms of the $N-1$ security standard. In particular, we implement both the proposed control strategy and the classical AGC [24] on the IEEE 118-bus testbed, and look at the average number of vulnerable lines across all the scenarios that lead to either successive failures or load shedding when they are tripped. In order to illustrate the improvements of the proposed control strategy in different levels of system congestion, we scale down the transmission line capacities to $\alpha = 0.9, 0.8, 0.7$ of the base values and collect statistics on the number of vulnerable lines in all these settings.

Our results are summarized in Fig. 6. It can be seen that the proposed control incurs far less number of vulnerable lines in all cases compared to AGC, and this difference is particularly clear when the system is congested. We highlight that this happens with the proposed control operates over the revised network, where some of the tie-lines are switched off and hence certain capacity is removed from the system. Moreover, the remaining tie-line (30, 38) in the revised network is never vulnerable under the proposed control.
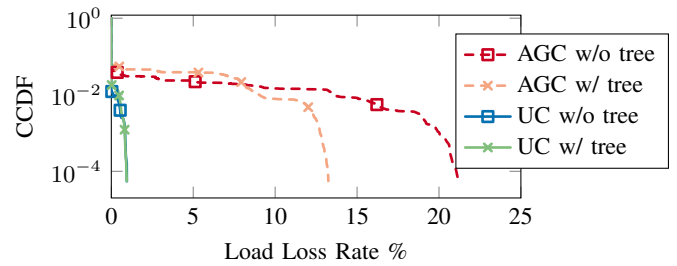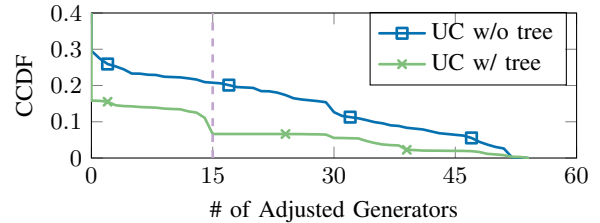
B. Loss of Load and Disruption to System Operation

We now look at the load loss rate, defined as the ratio between the total loss of load with respect to the original total demand, of the system to evaluate how well failures are mitigated in different settings. In this experiment, we scale down the generator capacities by 35% and the line capacities by 30% so that the system is more susceptible to failures. In order to demonstrate how UC and tree-partition impact the system performance seperately, we look at four different settings: (i) AGC on the original network; (ii) AGC on the revised network; (iii) UC on the original network; and (iv) UC on the revised network. Fig. 7 plots the complementary cumulative distribution (CCDF) of the load loss rates across all of the failure scenarios in these settings.

As one can see from the figure, for both the original and revised networks, UC significantly outperforms AGC. In particular, the largest load loss rate for UC is less than 2% for both networks, while AGC can lead to loss rate up to 14% on the revised network and 21% on the original network. This demonstrates the benefits of using our control strategy to mitigate failures.

Although the performance of UC in terms of loss rate are roughly the same with or without tree-partition, there is a drastic difference when we look at how well the failure impacts are localized. In Fig. 8, we plot the CCDF on the number of generators whose operating points are adjusted in response to the initial failures. It shows that the operation of much fewer generators is disrupted when the control areas that UC operates over form a tree-partition. This confirms our intuition and theoretical results about how a tree-partition structure helps localize failures.

VIII. Conclusion

In this work, we propose a control strategy that combines the concepts of the unified controller and the network tree-partition to mitigate and localize cascading failures in power system. Our case studies on the IEEE 118-bus test system show that the proposed control scheme greatly improves

system robustness to cascading failures as compared to classical AGC.

This work can be extended in several directions. First, our model builds upon linearized swing and power flow dynamics, which are accurate for small deviations but less so under large disruptions. It is of interest to understand how the non-linearity in more sophisticated models on large deviations impacts our results. Second, the proposed control strategy requires certain tie-lines to be switched off so that a tree-partition is formed. It would be useful if the selection of such lines can be systematically optimized under a certain objective function. Third, both the power flow redistribution and the line capacities are relevant in the cascading failure dynamics. It is important to investigate how adjustments on line capacities can be incorporated to our framework to further improve the system reliability.

REFERENCES

[1] D. Bienstock and S. Mattia, "Using mixed-integer programming to solve power grid blackout problems," *Discrete Optimization*, vol. 4, no. 1, pp. 115 – 141, 2007.

[2] P. Hines, S. Talukdar *et al.*, "Controlling cascading failures with cooperative autonomous agents," *International journal of critical infrastructures*, vol. 3, no. 1, p. 192, 2007.

[3] R. Baldick, B. Chowdhury, I. Dobson, Z. Dong, B. Gou, D. Hawkins, H. Huang, M. Joung, D. Kirschen, F. Li *et al.*, "Initial review of methods for cascading failure analysis in electric power transmission systems ieee pes cams task force on understanding, prediction, mitigation and restoration of cascading failures," in *2008 IEEE Power and Energy Society General Meeting-Conversion and Delivery of Electrical Energy in the 21st Century*. IEEE, 2008, pp. 1–8.

[4] B. A. Carreras, V. E. Lynch, I. Dobson, and D. E. Newman, "Critical points and transitions in an electric power transmission model for cascading failure blackouts," *Chaos: An interdisciplinary journal of nonlinear science*, vol. 12, no. 4, pp. 985–994, 2002.

[5] M. Anghel, K. A. Werley, and A. E. Motter, "Stochastic model for power grid dynamics," in *HICSS*. IEEE, 2007, pp. 113–113.

[6] J. Yan, Y. Tang, H. He, and Y. Sun, "Cascading failure analysis with DC power flow model and transient stability analysis," *IEEE TPS*, vol. 30, no. 1, pp. 285–297, 2015.

[7] A. Bernstein, D. Bienstock, D. Hay, M. Uzunoglu, and G. Zussman, "Power grid vulnerability to geographically correlated failures: Analysis and control implications," in *IEEE INFOCOM*, 2014, pp. 2634–2642.

[8] D. P. Nedic, I. Dobson, D. S. Kirschen, B. A. Carreras, and V. E. Lynch, "Criticality in a cascading failure blackout model," *International Journal of Electrical Power & Energy Systems*, vol. 28, no. 9, pp. 627–633, 2006.

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

[10] J. Song, E. Cotilla-Sanchez, G. Ghanavati, and P. D. Hines, "Dynamic modeling of cascading failure in power systems," *IEEE TPS*, vol. 31, no. 3, pp. 2085–2095, 2016.

[11] C. D. Brummitt, R. M. DSouza, and E. A. Leicht, "Suppressing cascades of load in interdependent networks," *Proceedings of the National Academy of Sciences*, vol. 109, no. 12, pp. E680–E689, 2012.

[12] Z. Kong and E. M. Yeh, "Resilience to degree-dependent and cascading node failures in random geometric networks," *IEEE TIT*, vol. 56, no. 11, pp. 5533–5546, Nov 2010.

[13] P. Crucitti, V. Latora, and M. Marchiori, "A topological analysis of the italian electric power grid," *Physica A: Statistical mechanics and its applications*, vol. 338, no. 1-2, pp. 92–97, 2004.

[14] I. Dobson, B. A. Carreras, and D. E. Newman, "A loading-dependent model of probabilistic cascading failure," *Probab. Eng. Inf. Sci.*, vol. 19, no. 1, pp. 15–32, Jan. 2005.

[15] Z. Wang, A. Scaglione, and R. J. Thomas, "A Markov-transition model for cascading failures in power grids," in *HICSS*. IEEE, 2012, pp. 2115–2124.

[16] M. Rahnamay-Naeini, Z. Wang, N. Ghani, A. Mammoli, and M. M. Hayat, "Stochastic analysis of cascading-failure dynamics in power grids," *IEEE TPS*, vol. 29, no. 4, pp. 1767–1779, 2014.

[17] P. D. Hines, I. Dobson, and P. Rezaei, "Cascading power outages propagate locally in an influence graph that is not the actual grid topology," *IEEE TPS*, vol. 32, no. 2, pp. 958–967, 2017.

[18] L. Guo, C. Liang, and S. H. Low, "Monotonicity properties and spectral characterization of power redistribution in cascading failures," in *Allerton Conference*, Oct 2017, pp. 918–925.

[19] L. Guo, C. Liang, A. Zocca, S. H. Low, and A. Wierman, "Failure localization in power systems via tree partitions," in *CDC*, Dec 2018, pp. 6832–6839.

[20] C. Zhao, E. Mallada, S. Low, and J. Bialek, "A unified framework for frequency control and congestion management," in *Power Systems Computation Conference (PSCC), 2016*. IEEE, 2016, pp. 1–7.

[21] C. Zhao, E. Mallada, S. H. Low, and J. Bialek, "Distributed plug-and-play optimal generator and load control for power system frequency regulation," *International Journal of Electrical Power & Energy Systems*, vol. 101, pp. 1–12, 2018.

[22] C. Zhao, U. Topcu, N. Li, and S. Low, "Design and stability of load-side primary frequency control in power systems," *Automatic Control, IEEE Transactions on*, vol. 59, no. 5, pp. 1177–1189, 2014.

[23] N. Li, C. Zhao, and L. Chen, "Connecting automatic generation control and economic dispatch from an optimization view," *IEEE Transactions on Control of Network Systems*, vol. 3, no. 3, pp. 254–264, 2016.

[24] A. R. Bergen, *Power systems analysis*. Pearson Education India, 2009.

[25] S. Soltan, D. Mazauric, and G. Zussman, "Analysis of failures in power grids," *IEEE TCNS*, no. 99, 2015.

[26] J. A. Bondy, U. S. R. Murty *et al.*, *Graph theory with applications*. Citeseer, 1976, vol. 290.

[27] L. Guo, C. Liang, A. Zocca, S. H. Low, and W. Adam, "Less is more: Real-time failure localization in power systems," *under preparation*.

[28] R. D. Zimmerman, C. E. Murillo-Sánchez, and R. J. Thomas, "Matpower: Steady-state operations, planning, and analysis tools for power systems research and education," *IEEE TPS*, vol. 26, no. 1, pp. 12–19, 2011.