IET Cyber-Physical Systems: Theory & Applications

Research Article

IET Journals
The Institution of Engineering and Technology

Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment

ISSN 2398-3396
Received on 30th January 2017
Revised 4th September 2017
Accepted on 14th September 2017
doi: 10.1049/iet-cps.2017.0014
www.ietdl.org

Shamina Hossain-McKenzie[1] ✉, Maryam Kazerooni[2], Katherine Davis[3], Sriharsha Etigowni[4], Saman Zonouz[4]

[1]*Electrical and Computer Engineering, University of Illinois at Urbana-Champaign, 306 N. Wright Street, Urbana, USA*
[2]*Appian Way Energy Partners, 25 Mount Auburn Street, Cambridge, USA*
[3]*Department of Electrical and Computer Engineering, Texas A&M University, 188 Bizzell Street, College Station, USA*
[4]*Department of Electrical and Computer Engineering, Rutgers University, 94 Brett Road, New Brunswick, USA*
✉ *E-mail: shossai2@illinois.edu*

Abstract: Cyber attacks and extreme events can cause severe consequences to the grid that require immediate response. Conventional remedial action schemes (RAS) use offline calculations to determine corrective control actions to deploy for a predetermined set of credible contingencies. Yet, cyber attacks cannot be sufficiently represented in a look-up table approach; such contingencies are highly dynamic and unpredictable. Online RAS with real-time calculation of corrective controls provides the most suitable and effective response. To achieve rapid computation and reduce the search space to only the most effective candidate control(s), the analytic corrective control selection method using clustering and factorisation techniques is developed based on controllability analysis. The resulting critical controls comprise a minimum set that is most effective in reducing the violations in the stressed areas of the system. While this study focuses on generators as the critical control mechanism, this methodology is broadly applicable to any corrective control for which a sensitivity matrix in relation to the violated components can be derived. The algorithm is evaluated with the IEEE 24-bus and IEEE 118-bus systems under compromised generator outage scenarios, and the identified critical control set is shown to be highly effective for reducing violations and improving RAS computation time.

1 Introduction

When abnormal conditions degrade the operational reliability and stability of a power system, corrective actions may be necessary. The North American Electric Reliability Corporation (NERC) defines a remedial action scheme (RAS) as 'an automatic protection system that detects those conditions and takes corrective actions to maintain system reliability, not limited to only component isolation' [1]. These actions may include changes to demand, generation, or system topology to maintain stability, acceptable voltage levels, and allowable power flows. Corrective actions are used to restore the power system's safe operation, details appear in [1–4].

Cyber attacks have become a serious concern. The Department of Homeland Security reported that from 2009 to 2014, about 40% of total critical infrastructure cyber incidents occurred in the energy sector [5]. In December 2015, one of the first publicised large-scale cyber attacks on a power grid occurred in Ukraine; this led to the disconnection of seven substations and power outage for 80,000 customers for several hours [6]. Power system cyber vulnerabilities have increased due to a number of modernisations, including the shift from proprietary control protocols to accessible network protocols. An adversary can exploit unsecured access points and potentially drive the power system to an unsafe state. Even more disconcerting is the ability of cyber attacks to cause physical damage to the grid, demonstrated in [7].

As the electric power grid is a complex, interconnected cyber-physical system, RAS procedures must be adapted to withstand malicious endeavours such as cyber attacks. Such response is critical to protect against the severe physical consequences that can result. Techniques that provide effective response are computationally efficient, and can be applied online during cyber attacks in large-scale power systems are the focus of this paper. Conventional RAS designs use offline calculations to determine which control actions to apply under credible contingencies and under multiple topology, generation, and load scenarios. These actions are subsequently stored and executed in real-time when the contingency occurs [8, 9]. Cyber attack contingencies cannot be accounted for in a look-up table due to their unpredictable nature and time-varying characteristics. Predefined tables also may not encompass all relevant states and require extensive data management. Online RAS based on the current system state and real-time calculation of corrective controls is the required response.

Computation time is paramount for online RAS. In the conventional RAS implementation, control actions are calculated for the post-contingency state and iterated through to determine the most suitable action; running time is not a significant concern. However, an online RAS design must be as fast as possible, as the corrective control must be executed immediately.

In the literature, there is a dearth of online RAS methods. Some strategies consider system dynamics when selecting corrective control actions [10–12]. Transient stability, while providing more thorough analysis, considerably increases computation time. A smart RAS scheme [13] developed by Wang and Rodriguez utilises synchrophasor-measurements of real power on tie-lines between two grid areas to trigger RAS. Motivated by intermittent renewable generation and load mutability, the authors design a no-parameter model and no-setting criteria to best predict and mitigate instability by effectively triggering RAS. Atighechi *et al.* [14] designed a fast load-shedding RAS method for British Columbia Hydro that applies dynamic and steady-state responses for various contingencies to best mitigate transient stability and voltage collapse.

Lastly, Hitachi is working with Bonneville power administration (BPA) to build [15] a new RAS prototype that uses synchrophasor input and online contingency analysis to account for new sources of power system disturbances from renewable energies and electric vehicles. The Hitachi-BPA design computes every 30 s and automatically calculates response actions against contingencies by using historical snapshots. The Hitachi-BPA project is the most prominent online RAS project to our knowledge, and it motivates the need and application of such

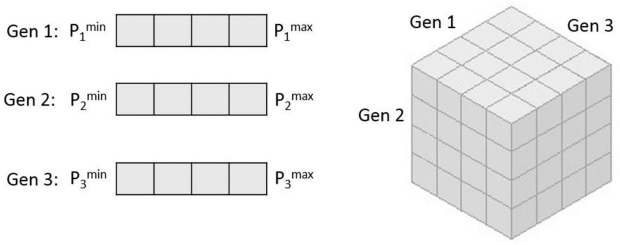

Fig. 1 *Security-compliant generator dispatch subspace synthesis*

designs. An automated RAS method was recently developed by Kazerooni [16] that contributes to that effort and applies steady-state analysis techniques to increase speed.

Dynamic performance and steady-state voltage sensitivity analysis at each bus in [14] determine a load-shedding sequence by a combination of those analyses, load level, load type, and system topology. Sensitivity analysis for control strategies against voltage collapse is applied by Song *et al.* [17]. Critical relays are identified whose operation significantly deteriorates the system's voltage stability. In both of these works, although sensitivities are used, controllability analysis concepts are not applied.

The proposed analytic corrective control selection (ACCS) algorithm for online RAS identifies the controls with the largest control span and thus the most significant impact on the violations in the stressed areas of the system. ACCS significantly improves RAS response computation time, indicating suitability for online application. As [16] is one of the few works that consider online RAS design and because full details of the algorithm are available, we utilise it to develop the ACCS algorithm in this paper.

This paper is organised as follows. A solution overview is first presented in Section 2, then the automated RAS is described in Section 3. The controllability-analysis-based ACCS formulation with online RAS is detailed in Section 4. The cyber-physical importance of the automated RAS scheme with ACCS is discussed in Section 5. Finally, evaluations are presented in Section 6 with the IEEE 24-bus case and the IEEE 118-bus case, and conclusions are provided in Section 7.

2 Solution overview

This paper enhances online RAS design with the proposed ACCS algorithm. ACCS provides an analytic critical control identification method for RAS. The identified controls are the most effective in reducing the violations at the various stressed areas of the system. The solution leverages sensitivities, considering the relationship between the corrective controls (e.g. generators) and the violations (e.g. overloaded lines). Clustering and factorisation are applied to analytically discover the critical controls. An assessment measure, the violation index, is also introduced to evaluate the operational reliability of the system following each action. This methodology is broadly applicable to any corrective control for which a sensitivity matrix in relation to the violated components can be derived.

The online RAS algorithm [16] employs a proximity-based critical generator identification (PCGI) method. Empirical studies indicate geographically clustered violations, so generators nearest to these stressed areas are identified as critical. Graph theory and proximity measures are applied to discover these generators, as described in Section 3.2. Although this method is effective in reducing the search space, it possesses several disadvantages:

- The number of critical generators must be specified a priori although a smaller set of critical generators may exist.
- The PCGI method is based on empirical analyses and may not apply to all systems and contingencies.
- The method neglects generators that are geographically distant from the violated areas.

As presented in the evaluations (Section 6), the ACCS algorithm not only utilises a lower number of critical generators than the proximity-based method but also achieves significant reduction of the violation index. When PCGI is set to the same number of resultant critical generators (termed modified PCGI or MPCGI), a different set is found and is still less effective at reducing the violation index. Therefore, ACCS is able to significantly reduce the computation time while also identifying the most broadly effective critical controls for all violations. With the inclusion of the ACCS algorithm in the online RAS design, fast and effective response is achieved.

The automated online response capability is also presented as a defense mechanism for maintaining system reliability when cyber attacks occur. Characterised as a large disturbance, generator outage(s) can have significant impact on the system that ranges from overloaded lines to loss of load to equipment damage. In the worst case, cascading effects can lead to blackout. Unplanned generator outages can be consequences of cyber attacks.

Two real-world examples of generator outages caused by cyber adversaries include the Ukraine event and the Aurora generator test. In the Ukraine scenario, cyber attackers, after gaining remote control of the SCADA distribution management system, caused unnecessary ‘scheduled’ maintenance outages of various generators associated with the targeted connected loads [6, 18]. In the 2007 Aurora generator test, researchers at Idaho National Laboratories demonstrated that using only cyber commands, they could cause a generator to explode. The command consisted of rapidly switching the generator's circuit breakers out of phase with the rest of the grid [7]. These scenarios demonstrate the serious physical consequences that can result from cyber attacks.

Effective response to cyber attacks requires actions in both the cyber and physical layers of the power grid. For example, a compromised, outaged generator must be ‘cleaned’ of the intrusion using cyber mechanisms such as intrusion detection and recovery systems. Meanwhile, the physical power system must react to maintain system reliability by maintaining continuous service, relieving stressed components, and preventing damage. A cyber-physical response (CPR) mechanism that employs both layers to respond to various contingencies is being developed within our research team [19]. In this paper, the calculation and application of cyber threat indices is presented in Sections 3.1 and 6.2.

Online RAS response would track the trajectory of a cyber attack and update the controls to maintain system reliability. In this manner, the proposed solution aids in defending the attacked system by responding with the most suitable remedial actions even as the attack is changing. The compromised generator outage scenario is examined in Section 6.

3 Automated remedial action scheme design

The automated RAS procedure developed by Kazerooni is briefly described in this section, with full details in [16]. For generation redispatch applications, the feasible control subspace of the power system with n generators is discretised into equally distant n-dimensional cubes, as shown in Fig. 1. Each point in the grid corresponds to one control action vector dependent on each generator's allowed dispatch MW range. The power flow is solved for each action and the resultant security constraints are evaluated. The actions that do not violate any constraints are identified as possible RAS solutions.

3.1 Proposed violation index

It is possible that no control actions can be taken that will satisfy all of the security constraints. In this case, the actions that violate fewer constraints and provide a more secure state are selected. A violation index may be defined to evaluate the resultant security of the system after an action. Aggregate MW overload (AMWCO), defined in [20], evaluates system security based on the total MW of line limit violations

$$\text{AMWCO} = \sum_{(i,j)\in\mathcal{F}} \max\{0, P_{ij}^{(k)} - P_{ij}^{\max}\} \tag{1}$$

where $P_{i,j}$ is the active power on the line between buses i and j, $P_{i,j}^{\max}$ is the flow limit of this line, and $\mathcal{F}$ is the set of all (i,j) for

1: **procedure** PCGI(Network State and Limits)
2: $\mathcal{U}^1_{CritBus}$ = Set of buses with violations
3: $\mathcal{U}^1_{CritGen} = \mathcal{U}_{PV} \cap \mathcal{U}^1_{CritBus}$
4: $k = 1$
5: **while** $Size(\mathcal{U}^k_{CritGen}) < CritGenMax$ **do**
6: $\mathcal{U}^k_{CritBus} = \mathcal{U}^{k-1}_{CritBus} \cup N(\mathcal{U}^{k-1}_{CritBus})$
7: $\mathcal{U}^k_{CritGen} = \mathcal{U}^{k-1}_{CritGen} \cup (\mathcal{U}_{PV} \cap \mathcal{U}^k_{CritBus})$
8: $k = k + 1$
9: **end while**
10: **end procedure**

Fig. 2 *Algorithm 1: Proximity-based critical generator identification*

which there is a line connecting bus i to bus j. This security index considers only line flow violations, and excludes bus voltage and generator power limits. To account for additional limit types, a general violation index is defined

$$\begin{aligned}\text{violation}^{(k)} = w_{\text{I}}S_{\text{I}}^{(k)} + w_{\text{V}}S_{\text{V}}^{(k)} + w_{\text{P}}S_{\text{P}}^{(k)} \\ + w_{\text{Q}}S_{\text{Q}}^{(k)} + w_{\text{Cy}}S_{\text{Cy}}^{(k)}\end{aligned} \tag{2}$$

where $S_{\text{I}}^{(k)}$, $S_{\text{V}}^{(k)}$, $S_{\text{P}}^{(k)}$, $S_{\text{Q}}^{(k)}$, $S_{\text{Cy}}^{(k)}$ are, respectively, the security indices of the line flows, bus voltages, generator active power outputs, generator reactive power outputs, and cyber threat level (defined in (4)) following action k. The corresponding weights w_{I}, w_{V}, w_{P}, w_{Q}, and w_{Cy} capture varying importance of the violation types. These weights are currently assigned heuristically, with greatest weights on generator limits. A systematic approach for assigning weights is left as future work. The security index for the line flows $S_{\text{I}}^{(k)}$ is given by

$$S_{\text{I}}^{(k)} = \sum_{(i,j) \in \mathcal{J}} \frac{\max\{0, P_{ij}^{(k)} - P_{ij}^{\max}\}}{P_{ij}^{\max}} \tag{3}$$

where the MW overloads are normalised by the line flow limits. Security indices $S_{\text{V}}^{(k)}$, $S_{\text{P}}^{(k)}$, $S_{\text{Q}}^{(k)}$ are also aggregate violations, normalised by upper bound limits. The violation index in this design is static; it assumes the power system is in quasi-steady state, though dynamic versions can be incorporated. As the current focus is to reduce computation time to develop RAS for online use, the static index is applied. Indices based on transient stability analysis and dynamic response may significantly increase calculation time, and future work will study how this can be improved.

The cyber threat index $S_{\text{Cy}}^{(k)}$ considers the ability of an attack to cause significant impact and also considers attack difficulty over a set of access paths. The index developed in the Cyber-Physical Security Assessment (CyPSA) for Electric Power Systems project [21] is part of a method and an open source platform for prioritising devices (i.e. protective relays) and the access paths to these devices. CyPSA specifically focuses on capturing attack impact and ease of attack. It is thus beneficial to adapt the same metric and computation for online RAS applications. Hence, the following cyber security violation index is proposed for this application

$$\begin{aligned}S_{\text{Cy}}^{(k)} = N \cdot (w_{\text{I}}S_{\text{I}}^{(k)} + w_{\text{V}}S_{\text{V}}^{(k)} + w_{\text{P}}S_{\text{P}}^{(k)} \\ + w_{\text{Q}}S_{\text{Q}}^{(k)}) \cdot C_{\text{EQ}}\end{aligned} \tag{4}$$

$$C_{\text{EQ}} = \frac{1}{\{\sum_{p(i) \in} (1/CC(p(i)))\}} \tag{5}$$

where A is the set of all access paths from an initial set of IP addresses or control network entry points to the end-devices connected to physical equipment (i.e. PLCs controlling generators) after action k. An access path $p(i)$ [21] indicates a multi-step sequence of vulnerability exploitations and compromised hosts that lead an adversary from the initial entry point to the targeted physical equipment. Since the physical impact portion of violation$^{(k)}$ is not dependent on the path taken to reach it, it is the same for all paths and appears in (4), multiplied by N, the number of paths in A. The cyber cost CC of a path $p(i)$ is based on the attack exploitability score, determined via CyPSA querying the National Vulnerability Database (NVD) with the list of ports and services that are running on each machine in the control network. The interpretation of the equivalent cost of a set of paths (5) is exactly the same as parallel resistors in a circuit. To compute and fully incorporate cyber-based metrics, a complete cyber-physical model of the system must be known, including the control network's access control policies and host vulnerability information. The authors are working to validate and improve online RAS using synthetic cyber-physical models while considering various threat profiles. This will appear as future work.

For the purposes of illustration of the method, and without loss of generality, the current paper adapts the synthetic control network model that was constructed for eight substations. The model was validated and released as part of the open source CyPSA and described in [22]. Section 6.2 details our evaluation using this coupled infrastructure model.

3.2 Proximity-based critical generation identification

The proximity-based PCGI method in [16] to which we compare ACCS is a greedy algorithm to identify insignificant generators based on graph theory and proximity measures. The computational complexity of control subspace synthesis is exponential in the number of participating generators. PCGI reduces the number of generators while still providing enough candidates to keep the performance near optimal. For every contingency, the lines and buses at which the constraints are violated are identified. The generators close to the areas under stress are classified as crucial and the ones which are further away are labelled as insignificant. 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 reach a user-specified value. Algorithm 1 (see Fig. 2) describes the procedure.

In Algorithm 1 (see Fig. 2), $\mathcal{U}^k_{\text{PV}}$ is the set of generator buses, $\mathcal{U}^k_{\text{CritBus}}$ and $\mathcal{U}^k_{\text{CritGen}}$ are, respectively, the set of critical buses and critical generators at level k, CritGenMax is the maximum number of critical generators defined by the user, and Size(x) returns the item count of set x. This heuristic technique provides acceptable results for the cases tested, but it does not provide the most effective critical generators, as discussed in Section 2. ACCS is designed to provide this analytic solution based on controllability analysis, subsequently identifying the most effective generators in *controlling* and thus reducing system stress from post-contingency overloads and other violations.

Computation time can be further reduced by using DC power flow (DCPF) instead of AC power flow (ACPF) for evaluating the impact of each possible action. Since DCPF is less accurate, it may be used as a fast screening tool before ACPF is applied to the top candidates.

4 Analytic corrective control selection

The proposed online RAS with ACCS leverages the sensitivities between the available corrective controls and the violated components. Clustering is performed to discover violation groups, and factorisation techniques are applied to identify the critical corrective controls. The algorithm is controllability analysis based, with rank conditions applied during the factorisation. The critical corrective control selection can be alternatively described as discovering the most effective controls in *controlling* the violated components and reducing the overall system stress.

The ACCS algorithm can be applied to any type of corrective control and violations, as long as the appropriate sensitivity matrix is computed. To aid in the explanation of the method, this paper utilises a generator outage example, where the violations are line overloads and the corrective controls are generators.

4.1 Sensitivities of critical controls and violations

A system's sensitivity matrix describes the relationships between components [23]. For generation redispatch, sensitivities provide insight into the interaction between available generators and violations. Considering generator outage(s) and line overload(s), the sensitivity of each line's real power flow to each available generator's real power changes is represented in the matrix $\mathbf{\Psi}$

$$\Delta \mathbf{P}_{\text{flow . line, overloaded}} = [\mathbf{\Psi}] \cdot \Delta \mathbf{G}_{\text{MW}} \tag{6}$$

With $\mathbf{\Psi}$, the sensitivities pertaining to the available generators and overloaded lines can be processed to discover which generators cause the greatest impact on the line flows. A subset of the sensitivity matrix is used in the current approach, where rows are associated with overloaded lines and columns with the available generators (excluding the slack bus and outaged generator(s)). The identified effective controls are then utilised in the enhanced automated RAS procedure.

4.2 Identifying independently controllable violations

After the sensitivities $\mathbf{\Psi}$ are obtained, ACCS clusters the rows to group the overloaded lines and determine which lines impact each other and which do not. The results of this step provide the following:

• *Violation groups*: for this paper, these are sets of overloaded transmission lines that can be controlled independently via generation redispatch.

Each violation group discovered is comprised of overloaded lines that impact each other significantly; they are highly coupled. Within each set, it only makes sense to target one overloaded line to control, as controlling one line flow will always strongly impact the others in a predictable way. The generator(s) selected to reduce the overload of that one line will also be effective for the rest of overloaded lines within the violation group. A different violation group will have different sensitivities and require calculation for generator(s) most effective for those overloaded lines. In this manner, a target set of overloaded lines, the most sensitive from each violation group, can be selected to further process and determine the critical generators that can provide the best corresponding control.

To determine these violation groups, we perform k-means clustering upon the cosine similarities between the different overloaded line sensitivities [24]. By comparing the angles between row vectors of $\mathbf{\Psi}$, the overloaded lines, the coupled and decoupled sets of overloaded lines and their real power flows are found. To calculate and compare these angles, we utilise the coupling index (CI) and measure the cosine similarity [24]. The CI is equal to the cosine of the angle between two row vectors, $\boldsymbol{v}_1$ and $\boldsymbol{v}_2$ of the sensitivity matrix $\mathbf{\Psi}$ as

$$\cos \theta_{\boldsymbol{v}_1 \boldsymbol{v}_2} = \frac{\boldsymbol{v}_1 \cdot \boldsymbol{v}_2}{\| \boldsymbol{v}_1 \| \| \boldsymbol{v}_2 \|} \tag{7}$$

The clusters, or violation groups, identified using the CI are approximately orthogonal to each other. The CI has values between −1 and 1. By clustering on the rows of the sensitivity matrix using CI, the coupled and decoupled sets of overloaded line flows can be determined. Thus, each cluster will be independent and decoupled from the other sets. Within the cluster, the line flows are coupled and dependent on one another.

For k-means clustering, we must provide k, the number violation groups we seek. However, we do not arbitrarily select k. Instead, our analytic solution determines the most suitable number of violation groups. This number is dependent on the system topology and current state. The resultant clusters should be highly cohesive; the overloaded lines within each violation group should exhibit similar responses to control.

To leverage the sensitivity matrix and its inherent groupings, the proposed ACCS method uses singular values that are computed from singular value decomposition (SVD). The SVD of a $m \times n$ matrix $\mathbf{\Psi}$ is

$$\mathbf{\Psi} = \boldsymbol{U} \mathbf{\Sigma} \boldsymbol{V}^{\mathrm{T}} \tag{8}$$

where $\boldsymbol{U}$ is an $m \times m$ orthogonal matrix, $\boldsymbol{V}$ is an $n \times n$ orthogonal matrix, and $\mathbf{\Sigma}$ is an $m \times n$ diagonal matrix with the singular values listed in decreasing order [25, 26]. The algorithm uses SVD to obtain a rank reduced approximation of the data set. Singular values and their associated vectors in $\boldsymbol{U}$ and $\boldsymbol{V}$ describe the controllers and measurements with the largest contributions to the matrix and its general structure. Therefore, the most significant or largest singular values represent the most significant groups present in the data matrix $\mathbf{\Psi}$.

Using the number of most significant singular values from the sensitivity matrix, ACCS achieves an initial guess for the number of clusters, k, for k-means clustering. To determine which singular values are most significant, ACCS calculates an *optimal hard threshold* using the techniques detailed by Gavish and Donoho, rigorously derived in [27], and henceforth referred to as the *hard threshold singular value* (HTSV) method. HTSV considers the recovery of low-rank matrices from noisy data by hard thresholding singular values. The HTSV thresholding rules adapt to the unknown rank and unknown noise level in an optimal manner and provide better results than truncated SVD (TSVD) [28]. The final result is not a fixed threshold chosen a priori but a data-dependent threshold, which is preferred for ACCS.

For a non-square $m \times n$ matrix with an unknown noise level, the optimal threshold value $\hat{\tau}^*$ is

$$\hat{\tau}^* = \omega(\beta) \cdot y_{\text{med}} \tag{9}$$

where y_{med} is the median singular value of the data matrix $\boldsymbol{Y}$ and the optimal hard threshold coefficient is dimension dependent ($\beta = (m/n)$) and calculated using a numerical formula, $\omega(\beta)$. If the matrix is square, $\omega(\beta)$ is simply replaced by $(4/\sqrt{3})$ [27].

4.3 Power system controllability

In power systems, the controllable region is the subset of the state space on which the available controls can be used to steer the power system from one state to any other state [29]. In general, the power system dynamical equation can be written as

$$\dot{\boldsymbol{x}} = f(\boldsymbol{x}) + \sum_{i=1}^{m} \boldsymbol{g}_i(\boldsymbol{x}) u_i, \ \boldsymbol{x} \in \mathbf{\Xi} \tag{10}$$

where $\boldsymbol{x}$ is an n-vector of dynamic variables (e.g. line power flows), $f(\boldsymbol{x})$ is a vector consisting primarily of the power flow equations, and $\sum_{i=1}^{m} \boldsymbol{g}_i(\boldsymbol{x}) u_i$ represents the effects of the controls on the system. The scalars $u_i, i = 1, \ldots, m$ are the system controls (e.g. generator real power injections) and are usually piece-wise constant in time, due to device physical characteristics. System state space, $\mathbf{\Xi}$, is an open subset of the n-dimensional Euclidean space. If $X(s_1, u, t) \in \mathbf{\Xi}$ represents the system movement with the initial state s_1, control u, and $0 \leq t \leq \infty$, the controllable region satisfies:

$$X(s_1, u, t) = s_2, \ u \in \boldsymbol{U} \text{ and } 0 \leq t \leq \infty \tag{11}$$

where every pair of states s_1 and $s_2 \in \boldsymbol{Z}$ satisfy (9). $\boldsymbol{Z}$ is the controllable region, a subset of $\mathbf{\Xi}$. Therefore, the system presented in (8) can be steered from a state to any other state within the controllable region. Further proofs and other references can be found in [29]. The set of controls is defined as the available generators in this work, and ACCS decomposes this set to identify the critical generators for use in online RAS.

With the clustered violation groups, ACCS selects one line from each group to form a target set of overloaded lines to process. Within each violation group, ACCS examines each overloaded line's average sensitivity to all available generators. The most sensitive overloaded line is selected to be included in the target set. Subsequently, the critical generators that are selected for this target set will be effective in reducing the violation index for all the

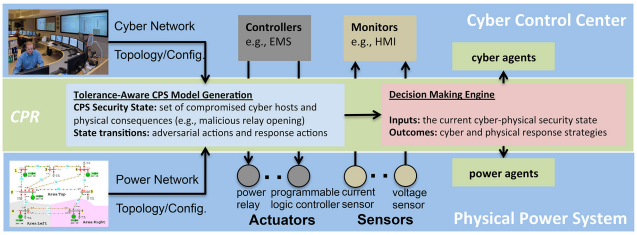

Fig. 3 *Cyber-physical intrusion tolerance with a minimal trusted computing base [19]*

overloaded lines. Furthermore, the sensitivities to be processed via factorisation are further reduced and computation time is lowered.

With the target set's sensitivity matrix, $\boldsymbol{\Psi}_{\mathrm{TAR}}$, with one overloaded line from each violation group in the rows and available generators in the columns, the factorisation method is applied to determine which of the generators are critical. These critical generators, defined below, are to be used with the automated RAS scheme, particularly with the continued example of generation redispatch after generator outage(s).

• *Critical generators*: for this paper, these are the minimum set of available generators needed to effectively respond to control the target overloaded lines and reduce violations.

The factorisation method inherently considers the coupling of the columns of $\boldsymbol{\Psi}_{\mathrm{TAR}}$ (or the rows of $\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}}$) to identify which generators will be most effective in reducing the violation index of the overloaded lines. This analysis is motivated by observability analysis-based algorithms that identify critical measurements to protect against false data injection attacks [30, 31]. Similarly, here controllability analysis is applied to determine which generators are essential in controlling the overloaded target lines, reducing the violation index.

4.4 Identifying a minimal spanning set of controls

To identify the critical generators, ACCS performs a change of basis that maps available generators to equivalent controllable states. The equivalent states are the real power flows of the overloaded lines. LU factorisation is applied to $\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}}$ to obtain the change of basis, decomposing the transposed sensitivity matrix to lower and upper triangular factors. Then, ACCS identifies the set of available generators needed to control those equivalent overloaded line flows and most effectively reduce the violation index through generation redispatch. The generation redispatch output quantities are found using the automated RAS procedure.

The following decomposition of $\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}}$ is obtained as

$$\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}} = \boldsymbol{P}^{-1}\boldsymbol{L}_{\mathrm{F}}\boldsymbol{U}_{\mathrm{F}} \tag{12}$$

$$\boldsymbol{L}_{\mathrm{F}} = \begin{bmatrix} \boldsymbol{L}_{\mathrm{b}} \\ \boldsymbol{M} \end{bmatrix} \tag{13}$$

Using the Peters–Wilkinson [32] method, ACCS decomposes $\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}}$ into its factors, where $\boldsymbol{P}$ is the permutation matrix and $\boldsymbol{L}_{\mathrm{F}}$ and $\boldsymbol{U}_{\mathrm{F}}$ are the lower and upper triangular factors of dimension n, respectively. $\boldsymbol{M}$ is a sparse, rectangular matrix with rows corresponding to the redundant generators. The new basis has the structure:

$$\boldsymbol{L}_{\mathrm{CER}} = \boldsymbol{L}_{\mathrm{F}}\boldsymbol{L}_{\mathrm{b}}^{-1} = \begin{bmatrix} \mathbf{G}_{\mathrm{CRIT}} \\ \mathbf{G}_{\mathrm{REM}} \end{bmatrix} \tag{14}$$

The transformed basis, shown in (12), must be full rank for a controllable system and this requires the $m \times (n-1)$ matrix to have a column rank of $(n-1)$ to be a controllable n-bus system with m-measurements [31]. Since $\boldsymbol{L}_{\mathrm{F}}$ and $\boldsymbol{U}_{\mathrm{F}}$ are non-singular for a controllable system, the rank of $\boldsymbol{\Psi}_{\mathrm{TAR}}^{\mathrm{T}}$ can be confirmed by checking the rank of the transformed factor $\boldsymbol{L}_{\mathrm{CER}}$. Also, $\boldsymbol{L}_{\mathrm{b}}$ has full rank, and with (12) multiplied by $\boldsymbol{L}_{\mathrm{b}}^{-1}$ from the right, the row identities are preserved in the transformed matrix $\boldsymbol{L}_{\mathrm{CER}}$. Each row of the transformed matrix therefore corresponds to the respective available generators [31].

Rows of $\boldsymbol{G}_{\mathrm{CRIT}}$ correspond to essential corrective controls, in this case generators, that are sufficient to assure independent controllability of the equivalent overloaded line flows. The rows of $\boldsymbol{G}_{\mathrm{REM}}$ correspond to the corrective controls that can be removed from the generation redispatch procedure. Columns correspond to the equivalent overloaded line flows which can easily be mapped back to the original flows using the permutation matrix $\boldsymbol{P}$ obtained from the LU decomposition step. These equivalent overloaded lines are composed of the target set of overloaded lines obtained from the clustered violation groups. The identified set of critical generators should be be used with the automated RAS scheme to reduce computation time significantly while effectively responding to geographically diverse line overloads.

5 Cyber-physical importance of control solutions

The importance of this work needs to be considered through its role as part of a system's cyber-physical intrusion response and recovery mechanisms (CPR) [19]. CPR has components to its solution at both micro- and macro-levels. Within CPR, it is intentional that we design physics-based solutions to prepare for, tolerate, and respond to cyber attacks. Physical means of defense are inherently agnostic to sources of threat. The more that physics can be integrated into the defense of power systems from cyber threats, the greater the assurance of defeating those threats. An adversary cannot control the underlying physics of the system under attack.

It is important to consider the control strategy in this paper as a foundational element of the system's overall cyber-physical intrusion tolerance and response design. In particular, ACCS improves the computation time as well as optimises and simplifies the inputs for the decision-making engine of CPR. Fig. 3 illustrates the coupled defense solution [19]. The work presented in this paper formulates a necessary control selection solution for enabling that framework and its realisation in practice.

CPR calculates the current cyber-physical security state of the infrastructure based on cyber intrusion detectors and power system measurements. The engine must then make decisions that drive optimal response and recovery strategies by recommending sequences of actions in both cyber and power system networks. Each decision must weigh the potential impacts on both environments. CPR is also a minimal-trusted computing base (TCB) [33] that minimises the attack surface exposed to adversaries who may attempt to subvert the deployed protections.

The automated RAS algorithm with ACCS plays a crucial role in responding to cyber attacks with fast and effective response that can be used for online post-contingency corrective control. Real-time post-contingency corrective control is necessary for cyber attacks as well as other extreme events where such events are not included in daily power systems planning and operations studies. The power system is not pre-emptively operated in a way that prevents violations in operational reliability and damage from these events. Online RAS with ACCS aids both intrusion detection and system recovery. Attack impact severity and trajectory are of great importance for how to operate a system under cyber attack. The violation index (defined in Section 3.1) quantitatively captures severity information and guides response though the life cycle of the attack or other extreme event. The choice and construction of an appropriate index in practice is influenced by availability of trustworthy data sources that measure violation severity. The violation index in this paper depends on the extent of violations of the physical, operating, and cyber security constraints of the system. After a generator outage occurs, we obtain a single violation index that represents the extent of these violations.

After deploying our response with the ACCS-enhanced online RAS, we can again examine the violation index to determine if the system has sufficiently recovered. As an attack progresses, the physical targets may be changing, and the violation index after each event can be used to observe the attack trajectory. The

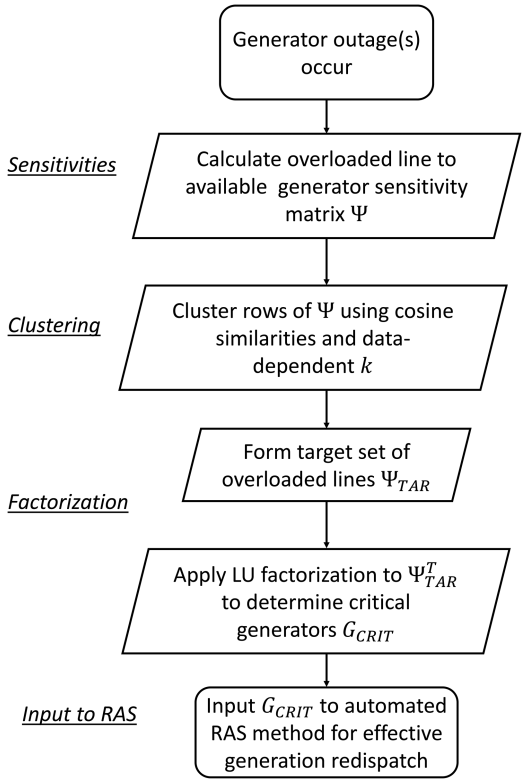

Fig. 4 *Flowchart of proposed ACCS method that uses clustering and factorisation to obtain critical generators to input to automated RAS design for generator outage(s) contingencies*

subsequent defense response after each step can also be observed, and a trajectory of the attack events and RAS responses can be analysed in the form of a violation index profile. This is described for the IEEE 24-bus case study in Section 6.

Therefore, the automated RAS algorithm with ACCS aids in the overall cyber-physical intrusion tolerance and response of the power system. It acts as a control strategy to minimise stress and damage to the system while responding to unpredictable cyber attacks in real-time, unlike existing designs that depend on offline calculation. The violation index profile provides further insight into cyber attacks. There is potential for detecting and categorising cyber attacks as well as employing game theory techniques to improve response in a cyber-adversarial environment. Cyber threat indices have also been developed and are applied for the IEEE 24-bus system in Section 6. To summarise, an automated RAS method with ACCS is a necessary and crucial building block in the overall cyber-physical security mechanism and allows for fast and effective response that can be computed online.

6 Evaluations

The ACCS method is summarised in the flowchart shown in Fig. 4. The ACCS algorithm is applicable to any contingency and violation for which a sensitivity matrix can be calculated that relates the available corrective controls to the violated components. For this paper, the example contingency of generator outage(s) and resultant overloaded lines is used and reflected in the flowchart.

As described in Section 2, generator outages are large disturbances that have significant impact on the power system. This paper focuses on such contingencies and the subsequent generation redispatch calculations to be computed by the presented ACC-enhanced online RAS design. Real-world cases such as the large-scale cyber attack on the Ukraine power grid and the Aurora generator test exemplify the severity of the consequences that could occur as well as how generators can be prominent targets for adversaries [6, 7, 18]. Therefore, when generator outages occur, from either benign or malicious sources, a quick and effective response is necessitated to maintain the system reliability via remedial actions. Both cyber and physical responses are required to respond to the attack. Cyber-defense mechanisms such as intrusion recovery systems must remove the compromise while physical control actions on the power system side must maintain grid operation and safety [19].

Table 1 IEEE 24-bus generator (Gen.) outage scenarios: resultant overloaded lines and violation index (Viol.)

Outage scenarios		
Outaged gen.(s)	Overloaded lines	Viol.
Gen.7	L1, L3, L12, L13	0.1421
Gen.23	L1, L3, L4, L5, L7, L8, L32	0.2183
Gen.7,13	L1, L2, L3, L5, L6, L26, L28, L33	0.6380

To ensure system reliability during a cyber attack with generation or load outage, the online RAS algorithm with ACCS enables automatic and immediate response that can be recalculated as the attack trajectory changes. Thus, as compromise is being investigated by cyber-physical security mechanisms, the effective generation redispatch response seeks to minimise stressed conditions and prevent damage to sensitive equipment. This response is demonstrated with the IEEE 24-bus and IEEE 118-bus systems for a cyber attack scenario with the following assumptions:

- A cyber adversary has gained access to certain generator controls through the energy management system and has caused the generator to shutdown, damage itself, or vary its output.
- The affected generators are now offline due to malicious compromise.
- Cyber-physical security mechanisms are investigating the conditions and seek to mitigate the compromise.
- While this is occurring, the enhanced RAS mechanism is maintaining system reliability by formulating the most effective generation redispatch.
- As the attack trajectory changes, the enhanced RAS mechanism is able to respond in near real-time.

To compute and fully incorporate cyber-based metrics, including the cyber threat index in Section 3.1, a complete cyber-physical model is essential. Such a model includes the control network's access control policies and vulnerability information of individually connected devices. Synthetic cyber-physical power system models are being developed independently. These models and metrics are proposed to be used in next steps by the authors to validate and improve online RAS while considering various threat profiles and attack scenarios.

6.1 IEEE 24-bus system

The ACCS algorithm is evaluated using the IEEE 24-bus system which has 11 generators and 38 lines. For this study, ACCS is used to identify the critical generators to be used in eliminating line overloads after the generator outage has occurred. The resultant critical generators are input to the automated RAS procedure. Three outage scenarios are considered, as presented in Table 1; the resultant overloaded lines and violation indices are listed. Additionally, lines operating at over 80% of their MVA line limits are also considered.

6.1.1 Generator 7 outage scenario: The first case considers an outage of generator 7 (Gen.7) and the subsequent line flow violations in Table 1. The post-contingency sensitivity matrix, $\boldsymbol{\Psi}$, is calculated for the four overloaded lines and nine available generators. These sensitivities reflect how each overloaded line's real power flow responds to each available generator's real power changes, as discussed in Section 4.

Next, ACCS clusters the rows of $\boldsymbol{\Psi}$ to obtain the violation groups. The CI calculation is applied to $\boldsymbol{\Psi}$ and the cosine similarities are clustered. To determine a data-dependent k for k-means clustering, SVD is applied to obtain the singular values, y_i, of $\boldsymbol{\Psi}$. These are listed in Table 2. The HTSV method by Gavish and Donoho [27] is utilised to determine the most significant

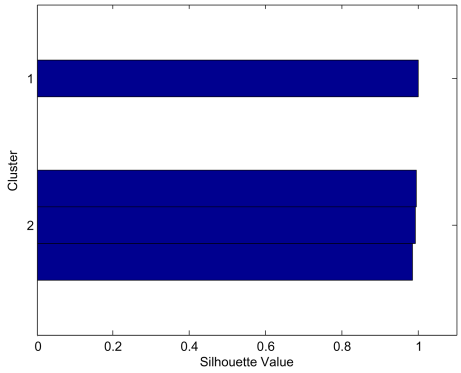

Fig. 5 *Silhouette values for overloaded lines in each violation group (clusters {1} and {2}) after Gen.7 outage*

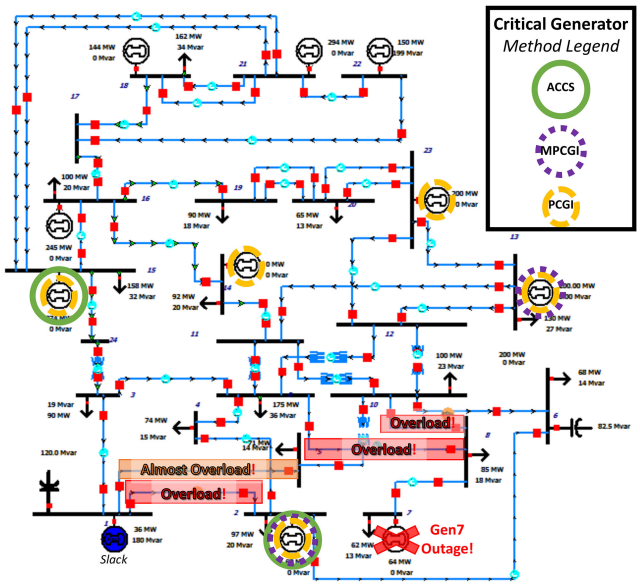

Fig. 6 *Gen.7 outage in the IEEE 24-bus system with overloaded and almost overloaded lines highlighted in red and the critical generators found by the ACCS, PCGI, and MPCGI methods labelled*

singular values. The algorithm, discussed in Section 4, outputs the following:

$$\hat{\tau}^{*} = \omega(\beta) \cdot y_{\text{med}} = 0.489 \tag{15}$$

We relax (15) slightly to include any y_i that are within 10% of the threshold. In this case, y_1 and y_2 satisfy the hard threshold, and we set $k = 2$. Next, Ψ is clustered using the k-means method with $k = 2$ and the cosine similarities. Two violation groups are obtained, as shown in Table 3.

Table 2 Singular values y_i of Ψ

*y*1	*y*2	*y*3	*y*4
1.7400	0.4590	0.0077	0.0180

Table 3 Violation groups {1} and {2} for Gen.7 outage

{1}	L1, L3, L12
{2}	L13

Table 4 IEEE 24-bus: Gen.7 outage results

	Viol.	Comp. time, s	$\boldsymbol{G}_{\text{CRIT}}$
ACCS	0.0371	0.5318	[2 15]
PCGI	0.0431	11.0171	[2 13 14 15 23]
MPCGI	0.0819	0.5828	[2 13]

Fig. 5 displays the resultant silhouette values from the clustering results. The silhouette technique is used to evaluate how well each object lies within its cluster. That is, silhouettes compare how similar an object is to the other objects in its cluster when compared with the objects in other clusters. The silhouette value, sil_i for the ith object, ranges from −1 to 1, thus the closer sil_i is to 1, the more well matched it is to its own cluster and poorly matched to neighbouring clusters [34]. The silhouette value for all four of our objects, the overloaded lines, are close to 1, and therefore indicate accurate clustering.

From the clustering results, the reduced set of sensitivities that includes only the target set of overloaded lines, $\boldsymbol{\Psi}_{\text{TAR}}$, is formulated. From {1}, L1 is the most sensitive overloaded line, and {2} has only one line, L13. Thus, $\boldsymbol{\Psi}_{\text{TAR}}$ is comprised of sensitivities of L1 and L13 to the nine available generators.

Then, $\boldsymbol{\Psi}^{\text{T}}_{\text{TAR}}$ is processed using LU factorisation to identify the critical generators, $\mathbf{G}_{\text{CRIT}}$, the minimum set of available generators needed to effectively respond to control the overloaded lines. For the Gen.7 outage, ACCS obtains the result:

$$\mathbf{G}_{\text{CRIT}} = [2\ 15] \tag{16}$$

Gen.2 and Gen.15 are critical and are input to the automated RAS algorithm to determine the generation redispatch settings. Table 4 and Fig. 6 summarises the results, where ACCS is compared with the PCGI method using five generators. The ACCS results are also compared with a modified PCGI (MPCGI) method in which the default was set to the data-dependent number of critical generators found by ACCS. The ACCS algorithm's ability to find the most effective generators to reduce the violation index is apparent.

The results indicate that the ACCS method was able to reduce the violation index (Viol.) most significantly (the original, post-contingency viol. is shown in Table 1). The PCGI method reduces the violation index acceptably but has a considerably larger computation time (Comp. Time, 0.5318 vs. 11.071 s). When the proximity-based method, MPCGI, is set to the same number of critical generators in ACCS's $\boldsymbol{G}_{\text{CRIT}}$, the violation index has not been reduced as effectively. The proximity-based method only considers the nearby generators and does not find the most effective generators to respond to the line overloads. The ACCS algorithm considers the whole set of available generators to obtain the critical set. Of the total computation time (Comp. Time), the calculation of the critical generators by ACCS, PCGI, or MPCGI are all under 1 s, and therefore add minimal overhead to the RAS algorithm.

6.1.2 Generator 23 outage scenario: The Gen.23 outage scenario results are also presented in Table 5. It can be observed that ACCS finds a much smaller critical generator set (Gen.2 and Gen.15) while achieving a low violation index and fast computation time. PCGI achieves a similar (slightly better) reduction of the violation index, but does so with five critical generators and, thus, a much longer generation redispatch calculation. MPCGI has the fastest computation with two critical generators, as found by the ACCS method, but has the worst performance and does not reduce the violation index significantly.

6.1.3 Double outage scenario: The results for the double outage of Gen.7 and Gen.13 are shown in Table 6 and Fig. 7. In this case, the ACCS method has the best performance in selecting the most effective critical generators. The PCGI algorithm performs fairly well, but at the expense of excessive computation time. The MPCGI method does not select the most effective critical generators and, therefore, has the least reduction in violation index.

6.2 Evaluation of cyber attack trajectory and state

A violation index profile is shown in Fig. 8 for the IEEE 24-bus system. The adversary's attack may be state dependent, where the attack is carried out based on the defending system's response. Large power swings could be induced by the attacker outaging

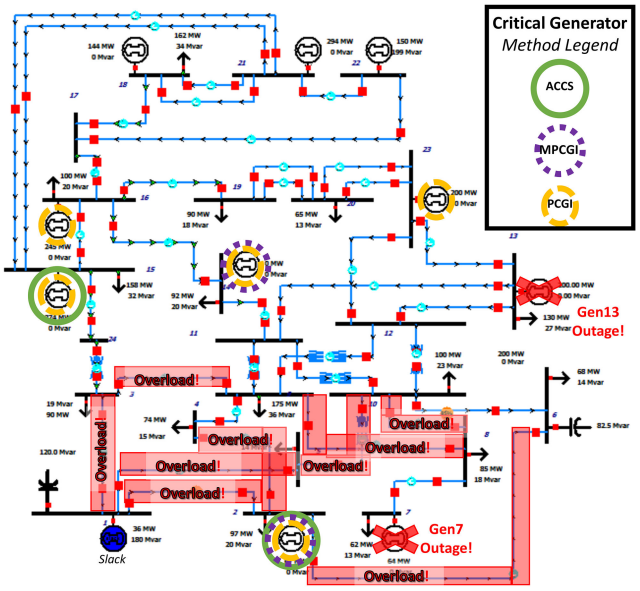

Fig. 7 *Gen.7 and Gen.13 outage in the IEEE 24-bus system with overloaded lines highlighted in red and the critical generators found by the ACCS, PCGI, and MPCGI methods labelled*

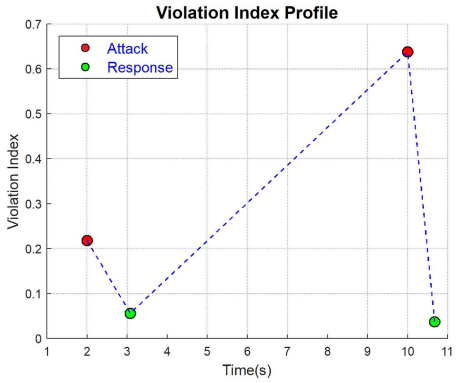

Fig. 8 *Violation index profile showing the trajectory of a cyber attack in IEEE 24-bus system: a single outage occurs at 2 s with a violation index of 0.2183 and the subsequent response of RAS with ACCS 1.077 s later reduces the violation to 0.056; next, a double outage occurs at 10 s with a violation index of 0.6380 and RAS with ACCS responds after 0.673 s and reduces it to 0.037*

generator(s) and the automated RAS increasing generation and could eventually destabilise the system. This response-dependent attack can be described as a Stackelberg game in which the adversary and defender have varying reward functions. Attack signatures can be defined based on the trajectories and used to detect cyber attacks. For example, geographically distant generators with correlated outages may indicate malicious activity. Geographic information of outages and violations would benefit detection efforts. The violation index profile would aid in studying

Table 5 IEEE 24-bus: Gen.23 outage results

	Viol.	Comp. time, s	G_{CRIT}
ACCS	0.0562	1.0765	[2 15]
PCGI	0.0517	11.0692	[2 13 14 15 23]
MPCGI	0.1472	0.6146	[2 7]

Table 6 IEEE 24-bus: Gen.7 and Gen.13 outage results

	Viol.	Comp. time, s	G_{CRIT}
ACCS	0.0371	0.6734	[2 15]
PCGI	0.0489	14.3243	[2 14 15 16 23]
MPCGI	0.0819	0.5818	[2 14]

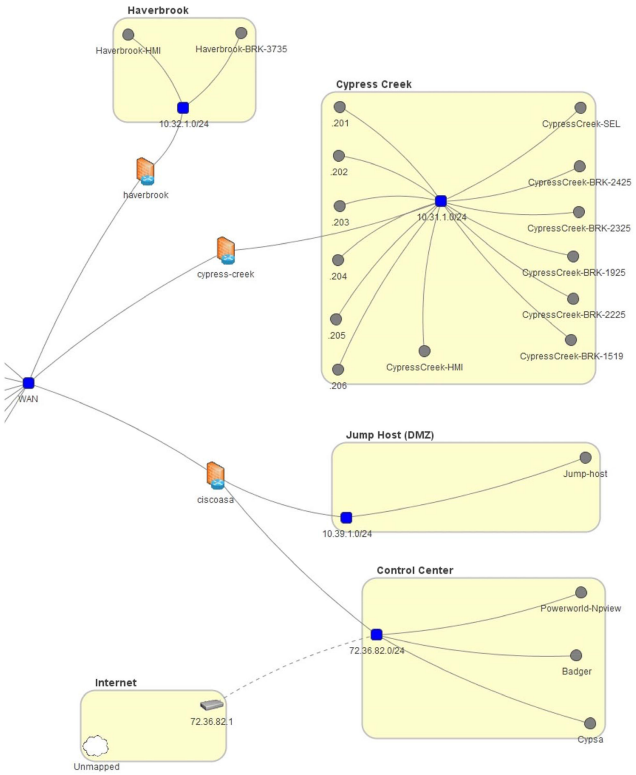

Fig. 9 *Cyber topology of a control network behind firewalls*

the attacker's reward function to determine his or her goals and would thus inform how the defender should alter his or her response. This cyber attack model is discussed in [19].

To illustrate how cyber state data is used with online RAS, we adapt the cyber network topology consisting of network devices (e.g. switches or routers) as well as controllers (e.g. programmable logic controllers) as shown in Fig. 9. Then, the cyber cost for the system on each path is calculated using CyPSA tool Armadillo [35] based on (4). Substations Cypress Creek and Haverbrook are IP connected, with generator controllers behind the firewall. The cyber cost is calculated based on the vulnerabilities present in the devices and the path an adversary would need to traverse ((4) and (5)). The vulnerabilities are obtained from the NVD. The common vulnerability scoring system is used to calculate the severity of the vulnerability. The cyber cost is calculated for all the devices in the topology, and the cyber cost to reach the devices that are directly controlling the generators are shown in Table 7. In this control network topology, the network paths to the generators are equivalent and the generator controllers are the same, so the cyber cost to reach each generator from any given attack entry point is the same. Thus, Table 7 gives the cyber costs for starting IP addresses in each area of the control network; locations are Cypress Creek and Haverbrook substations, the demilitarised zone (DMZ), and the control centre. An attack starting in the DMZ is found to have the lowest cost and thus the highest violation index. Variations in cyber topologies and threat profiles will be investigated in future work. The cyber cost is used in calculating the overall cyber-physical violation index. The security violation index prioritises protection against cyber-physical attacks. The security violation index can be used to direct control operations as well as to justify protection mechanisms like network-based intrusion detection systems that protect vulnerable cyber devices against attack.

6.3 IEEE 118-bus system

The IEEE 118-bus system in Fig. 10 was also tested with the compromised generator scenario shown in Table 8. The system has 54 generators and 186 lines. Evaluations for this system consider generator outage and line overloads, specifically the outage of Gen.10, which results in the largest violation index.

Table 7 IEEE 24-bus: Cyber Cost Calculations

Compromised IP address	IP address location	Num. paths	Path cost	C_{EQ} (5)
10.31.1.201	Cypress Creek	5	7.952	1.5904
10.32.1.250	Haverbrook	1	6.832	6.832
10.39.1.22	DMZ	6	8.5888	1.4315
72.36.82.194	Control Centre	6	17.1776	2.8629

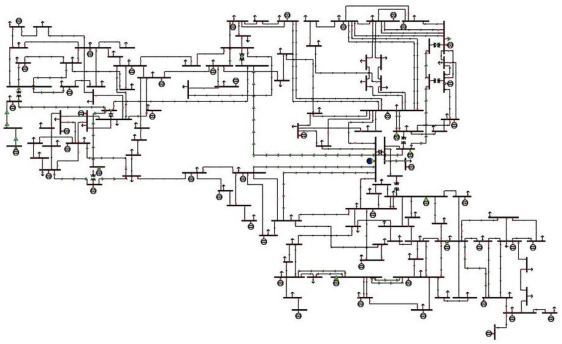

Fig. 10 *IEEE 118-bus case with 54 generators and 186 lines*

Table 8 IEEE 118-bus generator (Gen.) outage scenarios: resultant overloaded lines and violation index (Viol.)

Outage scenarios		
Outaged gen.(s)	Overloaded lines	Viol.
Gen.10	L21, L33, L37, L40, L57, L63, L66, L70, L85, L123	1.257

Table 9 IEEE 118-bus: Gen.10 outage results

	Viol.	Comp. time, s	G_{CRIT}
ACCS	0.0751	1.8110	[4 36 49 73]
PCGI	0.0928	5.3096	[8 15 18 19 24 25 32 34]
MPCGI	0.1149	1.7704	[8 15 18 19]

The results, shown in Table 9, indicate that the ACCS algorithm selected the most effective critical generators for reducing the violations. Using only four critical generators, the violation index was reduced from the original 1.257 to 0.0751. The default number of critical generators was set to eight generators in the PCGI method. The PCGI algorithm was able to achieve acceptable reduction of the violation index but with significantly larger computation time. Finally, the MPCGI method, set to the same number as ACCS as discovered through clustering, obtains similar computation time (as expected) but suffers in performance with the least reduction in the violation index.

7 Conclusion

Offline RAS calculations and look-up tables do not suffice for unpredictable events such as cyber attacks. To address this shortcoming, this paper presents solutions to support online RAS through real-time computation of corrective controls, where the resultant controls are determined based on the current system state and designed to provide the most suitable and effective response. An algorithm is presented to select the most effective corrective controls to use with online RAS, significantly reducing computation time. The resulting online RAS can respond automatically and effectively even as the attack trajectory changes.

The ACCS method developed in this work is a controllability analysis-based formulation that leverages sensitivities and applies clustering and factorisation techniques. In this manner, the critical corrective controls are identified to be the most effective in reducing violations in stressed areas of the system and are the minimum set. Compromised generator outage(s) in the IEEE 24-bus and IEEE 118-bus systems are studied, and the critical generators selected by ACCS provide significant reduction in the violation index. Only a fraction of the available generators is needed, and the computation time of RAS is made much faster. ACCS finds the most effective minimal set of critical corrective controls for RAS helps to restore the system to a normative state while undergoing a cyber attack. The negligible computation overhead by ACCS and subsequent speed-up of RAS calculations is promising for online applications. Furthermore, the enhanced RAS design's crucial pairing with cyber threat indices was demonstrated.

This work can be further extended to utilise DCOPF or ACOPF improvements to the RAS formulations to reduce computation time, as formulations that maximise reliability lead to longer computation times [36]. An interesting future direction would explore a systematic approach for selecting weights for the violation metrics and sensitivity elements while considering multiple types of simultaneous violations.

8 Acknowledgment

The authors thank the National Science Foundation (NSF) under Award Numbers CNS 1446229 and CNS 1446471 and ARPA-E under Award Number DE-AR0000233 for their support and sponsorship of this research.

9 References

[1] North American Electric Reliability Corporation: 'Proposed definition of 'remedial action scheme', NERC Reliability Standards. Available at http://www.nerc.com/pa/Stand/Prjct201005_2SpclPrtctnSstmPhs2/Proposed%20RAS%20Definition_10262014_clean.pdf

[2] Meliopoulos, A.P., Bakirtzis, A.G.: 'Corrective control computations for large power systems', *IEEE Trans. Power Appar. Syst.*, 1983, **PAS-102**, (11), pp. 3598–3604

[3] Anderson, P.M., LeReverend, B.K.: 'Industry experience with special protection schemes', *IEEE Trans. Power Syst.*, 1996, **11**, (3), pp. 1166–1179

[4] Henville, C.F., Struyke, E.: 'RAS and stretched power system'. Western Protective Relaying Conf., 2006

[5] Wirfs-Brock, J.: 'The realities of cybersecurity at a rural utility', Inside Energy, September 2015. Available at http://grid.insideenergy.org/cybersecurity/

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

[7] Liu, C.C., Stefanov, A., Hong, J., *et al.*: 'Intruders in the grid', *IEEE Power Energy Mag.*, 2012, **10**, (1), pp. 58–66

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

[9] Pai, S.C., Sun, J.: 'BCTCs experience towards a smarter grid—increasing limits and reliability with centralized intelligence remedial action schemes'. Electric Power Conf., 2008. EPEC 2008. IEEE, Canada, October 2008, pp. 1–7

[10] Fouad, A.A., Ghafurian, A., Nodehi, K., *et al.*: 'Calculation of generation-shedding requirements of the B.C. hydro system using transient energy functions', *IEEE Power Eng. Rev.*, 1986, **PER-6**, (5), pp. 31–32

[11] Zhang, Y., Tomsovic, K.: 'Adaptive remedial action scheme based on transient energy analysis'. Power Systems Conf. Exposition, 2004. IEEE PES. IEEE, 2004, pp. 925–931

[12] Shao, W., Vittal, V.: 'Corrective switching algorithm for relieving overloads and voltage violations', *IEEE Trans. Power Syst.*, 2005, **20**, (4), pp. 1877–1885

[13] Wang, S., Rodriguez, G.: 'Smart RAS (remedial action scheme)'. 2010 Innovative Smart Grid Technologies (ISGT), January 2010, pp. 1–6

[14] Atighechi, H., Hu, P., Lu, J., *et al.*: 'A fast load shedding remedial action scheme using real-time data for BC hydro system'. 2016 IEEE Power and Energy Society General Meeting (PESGM), July 2016, pp. 1–5

[15] L. Hitachi America: 'Introduction to online RAS (remedial action scheme)', April 2016. Available at https://www.wecc.biz/Administrative/RAS%20Arming%20-%20Hitachi%20America.pdf

[16] Kazerooni, M.: 'Enhanced power system resiliency to high-impact, low-frequency events with emphasis on geomagnetic disturbances'. PhD dissertation, University of Illinois at Urbana-Champaign, 2016

[17] Song, H., Lee, B., Ajjarapu, V.: 'Control strategies against voltage collapse considering undesired relay operations', *IET. Gener. Transm. Distrib.*, 2009, **3**, (2), pp. 164–172

[18] Lee, R.M., Assante, M.J., Conway, T.: 'Analysis of the cyber attack on the Ukrainian power grid', *SANS Ind. Control Syst.*, 2016

[19] Hossain, S., Etigowni, S., Davis, K., *et al.*: 'Towards cyber-physical intrusion tolerance'. 2015 IEEE Int. Conf. Smart Grid Communications (SmartGridComm), 2015, pp. 139–144

[20] 'D-FACTS devices in PowerWorld Simulator.' Available at https://www.powerworld.com/files/PW-DFACTS-QuickStart-Jan-15-2014.pdf

[21] Davis, K.R., Berthier, R., Zonouz, S.A., *et al.*: 'Cyber-physical security assessment (CyPSA) for electric power systems', *IEEE-HKN: The Bridge*, 2016, **112**, (2), pp. 8–19, an optional note
[22] Weaver, G.A., Davis, K., Davis, C.M., *et al.*: 'Cyber-physical models for power grid security analysis: 8-substation case'. 2016 IEEE Int. Conf. Smart Grid Communications (SmartGridComm), November 2016, pp. 140–146
[23] Dahleh, M., Diaz-Bobillo, I.: '*Control of uncertain systems: a linear programming approach*' (Prentice Hall, 1995)
[24] Rogers, K.M., Klump, R., Khurana, H., *et al.*: 'An authenticated control framework for distributed voltage support on the smart grid', *IEEE Trans. Smart Grid*, 2010, **1**, (1), pp. 40–47
[25] Heath, M.T.: '*Scientific computing*' (McGraw-Hill, New York, 2002)
[26] Lim, J.M., DeMarco, C.L.: 'Model-free voltage stability assessments via singular value analysis of PMU data'. Bulk Power System Dynamics and Control—IX Optimization, Security and Control of the Emerging Power Grid (IREP), 2013 IREP Symp., August 2013, pp. 1–10
[27] Gavish, M., Donoho, D.: 'The optimal hard threshold for singular values is $(4/\sqrt{3})$', *IEEE Trans. Inf. Theory*, 2014, **60**, (8), pp. 5040–5053
[28] Golub, G., Kahan, W.: 'Calculating the singular values and pseudo-inverse of a matrix', *J. Soc. Ind. Appl. Math. B Numer. Anal.*, 1965, **2**, (2), pp. 205–224
[29] Hong, M., Liu, C.-C.: 'Complete controllability of power system dynamics'. The 2000 IEEE Int. Symp. Circuits and Systems, 2000, vol. **4**, pp. 241–244
[30] Bobba, R.B., Rogers, K.M., Wang, Q., *et al.*: 'Detecting false data injection attacks on dc state estimation'. Preprints of the First Workshop on Secure Control Systems, CPSWEEK, 2010
[31] Chen, J., Abur, A.: 'Placement of PMUs to enable bad data detection in state estimation', *IEEE Trans. Power Syst.*, 2006, **21**, (4), pp. 1608–1615
[32] Peters, G., Wilkinson, J.H.: 'The least squares problem and pseudo-inverses', *Comput. J.*, 1970, **13**, (3), pp. 309–316
[33] United States Department of Defense: 'Trusted computer system evaluation criteria (orange book)', Technical Report 1985
[34] Rousseeuw, P.J.: 'Silhouettes: a graphical aid to the interpretation and validation of cluster analysis', *J. Comput. Appl. Math.*, 1987, **20**, pp. 53–65
[35] CyPSA Team, Information Trust Institute, University of Illinois: 'Cypsa open source release', https://github.com/bigezy/Armadillo, 2016
[36] Hug-Glanzmann, G., Andersson, G.: 'Decentralized optimal power flow control for overlapping areas in power systems', *IEEE Trans. Power Syst.*, 2009, **24**, (1), pp. 327–336