Received: 16 October 2019 | Revised: 10 September 2020 | Accepted: 22 January 2021 | IET Cyber-Physical Systems: Theory & Applications

DOI: 10.1049/cps2.12006

The Institution of Engineering and Technology WILEY

ORIGINAL RESEARCH PAPER

Strategy for distributed controller defence: Leveraging controller roles and control support groups to maintain or regain control in cyber-adversarial power systems

Shamina Hossain-McKenzie[1] | Kaushik Raghunath[2] | Katherine Davis[2] | Sriharsha Etigowni[3] | Saman Zonouz[4]

[1]Cyber Resilience R&D Department, Sandia National Laboratories, Albuquerque, NM, USA

[2]Department of Electrical and Computer Engineering, Texas A and M University, College Station, Texas, USA

[3]Department of Computer Science, Purdue University, West Lafayette, Indiana, USA

[4]Department of Electrical and Computer Engineering, Rutgers University, New Brunswick, NJ, USA

Correspondence

Shamina Hossain-McKenzie, Cyber Resilience R and D Department, Sandia National Laboratories, Albuquerque, NM, USA.
Email: shossai@sandia.gov

Funding information

National Science Foundation, Grant/Award Numbers: CNS 1446229 and CNS 1446471; U.S. Department of Energy, Grant/Award Number: CEDS DE-0E0000895

Abstract

Distributed controllers play a prominent role in electric power grid operation. The coordinated failure or malfunction of these controllers is a serious threat, where the resulting mechanisms and consequences are not yet well-known and planned against. If certain controllers are maliciously compromised by an adversary, they can be manipulated to drive the system to an unsafe state. The authors present a strategy for distributed controller defence (SDCD) for improved grid tolerance under conditions of distributed controller compromise. The work of the authors' first formalises the roles that distributed controllers play and their control support groups using controllability analysis techniques. With these formally defined roles and groups, the authors then present defence strategies for maintaining or regaining system control during such an attack. A general control response framework is presented here for the compromise or failure of distributed controllers using the remaining, operational set. The SDCD approach is successfully demonstrated with a 7-bus system and the IEEE 118-bus system for single and coordinated distributed controller compromise; the results indicate that SDCD is able to significantly reduce system stress and mitigate compromise consequences.

1 | INTRODUCTION

The smart grid initiative has facilitated increasingly sophisticated systems of sensors, algorithms, and controllers that are involved in widespread communication and online decision-making. These systems, which improve the operating efficiency of the grid, can also make the grid more susceptible to unsafe operation under attacks or failures. In this work, *distrusted control* is a situation where one or more controllers are compromised and under the command of a sophisticated adversary. Such an adversary is able to craft commands in a legitimate format and thus have them successfully executed in the system. Furthermore, these alterations can be invisible to the operator and automated security systems; about 59% of power and utility companies reported a recent significant cybersecurity incident in EY's Global Information Security Survey for 2016–2017 [1]. The threat of physical consequences resulting from these cyber-attacks is a serious concern, raising attention through demonstration in [2, 3]. One of the first publicised large-scale attacks on a power grid occurred in December 2015 in Ukraine. This attack led to disconnection of seven substations and power outage for more than 200,000 customers for several hours [4]. A second Ukraine attack in 2016 is attributed to malware CrashOverride, which, as reported by Dragos Security, is specifically designed and deployed to attack electric grids [5].

As modern power systems are increasingly outfitted with publicly available operating systems, network communications, and third-party software, a myriad of access points may exist through which an adversary may enter. The benefit of 'security

by obscurity' does not exist. A motivated adversary need not possess deep knowledge of a specific utility system to launch a successful attack [6]. In preventing and mitigating attacks, it is essential to consider feasible attack vectors, adversary capabilities, trusted entities, and the impact of these on system controllability and stability.

Existing research in the distributed control domain focuses predominately on methods to control diverse sets of resources such distributed energy resources (DERs) for microgrids [7]. Additionally, methods to divide global control tasks among DERs and other units are of great interest. Distributed control is also being investigated for specific goals such as frequency control or voltage support using agent-based technologies [8, 9]. These efforts are integral for modernising and achieving a smarter grid, but the focus is on the control architecture and tasks. Here, we present a general method for characterising a controller set and utilising those characteristics to respond to system disturbances, including controller compromise.

This paper presents *the systematic formulation of controller-based defences against controller-based attacks* in power systems. In particular, a strategy for distributed controller defence (SDCD) is developed that leverages power system interconnectivity and controllability knowledge to enable operators or automated defence solutions to restore the control capability of a system following such an attack. SDCD employs the residual set of functional controllers in proactive distributed controller response strategies where controllers reinforce other controllers by taking advantage of the naturally occurring redundancy in the meshed transmission network to maintain or regain control of the system given coordinated compromise or failure.

The high-level architecture and background for SDCD is presented in Section 2. The distributed controller role and interaction discovery (RID) analysis utilised in SDCD is provided in Section 3, and its application for offline analysis is detailed in Section 4. The online SDCD method is presented in Section 5, demonstrating its ability to respond to controller compromise. In Section 6, the state dependence of the results is analysed. Section 7 provides results and discussion for the 7-bus and IEEE 118-bus systems for single and coordinated distributed controller compromise. Section 8 concludes the paper.

2 | OVERVIEW OF SDCD FRAMEWORK

An overview of SDCD is given in Figure 1.

The strategy leverages the distributed controller RID algorithm [10, 11] to classify controllers into control support groups and controller roles which are then applied to maintain control of the system during an attack, where the attacks of interest are those that manipulate the output of other controllers. The contribution of this paper is to close the loop by using these roles and groups to develop a coordinated response strategy to distributed controller compromise, as shown in Figure 1. This work addresses a critical need for coordinated response in achieving cyber-physical intrusion tolerance by providing a strategy for distributed control response that

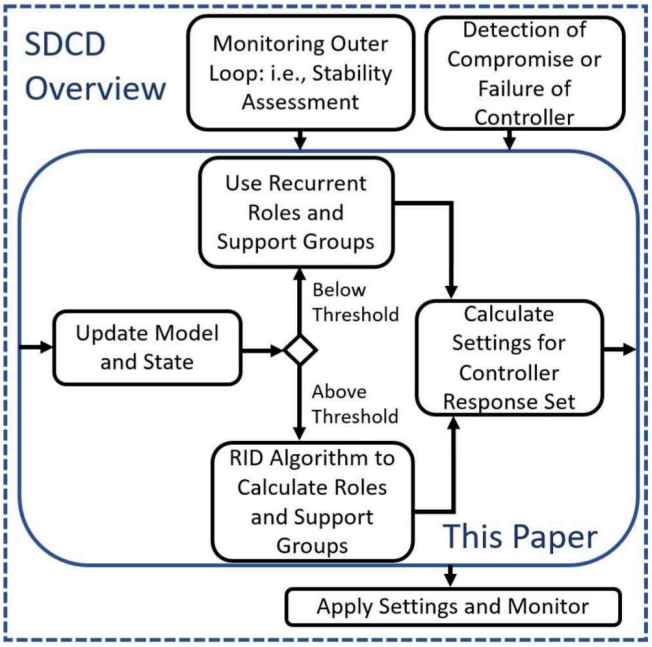

FIGURE 1 Functional overview of SDCD that analyses power system distributed controllers to allocate monitoring resources, to inform design decisions to strengthen system control, and to quickly, effectively respond during an attack with residual controllers

involves study of how often roles/groups need to be calculated, mapping equivalent line flows, ranking redundant controllers, computation of control settings, and demonstration and evaluation of coordinated distributed controller response on the presented test systems. The sensitivity-based roles in SDCD provide both (1) ahead-of-time controller placement to avoid loss of system controllability as well as and (2) online algorithms to formulate the most effective response with the non-compromised controllers. The application of SDCD is illustrated with a set of 10 distributed controllers in Figure 2.

2.1 | Motivation

Multiple strategically compromised and manipulated controllers can cause severe impact, and they may be able to drive the power system to an unsafe or unreliable operating state. While conventional attacks on the grid observed so far have primarily been forms of disconnection of key elements to force the grid to shut down, sophisticated attacks, such as the ones discussed in this paper are possible by a more knowledgeable and motivated attacker. For example, an insider threat may have goal(s) that are not to just make the grid succumb to an attack, but to degrade operation steadily, primarily motivated by economic factors. Such attacks could be developed to make system operation more expensive, increase congestion at desired locations, or spoof misoperation of specific devices so as to influence decisions such as vendor selection.

Distributed controller attack vectors include execution of malicious commands to damage to sensitive equipment, forced controller settings, or topology changes that intentionally create

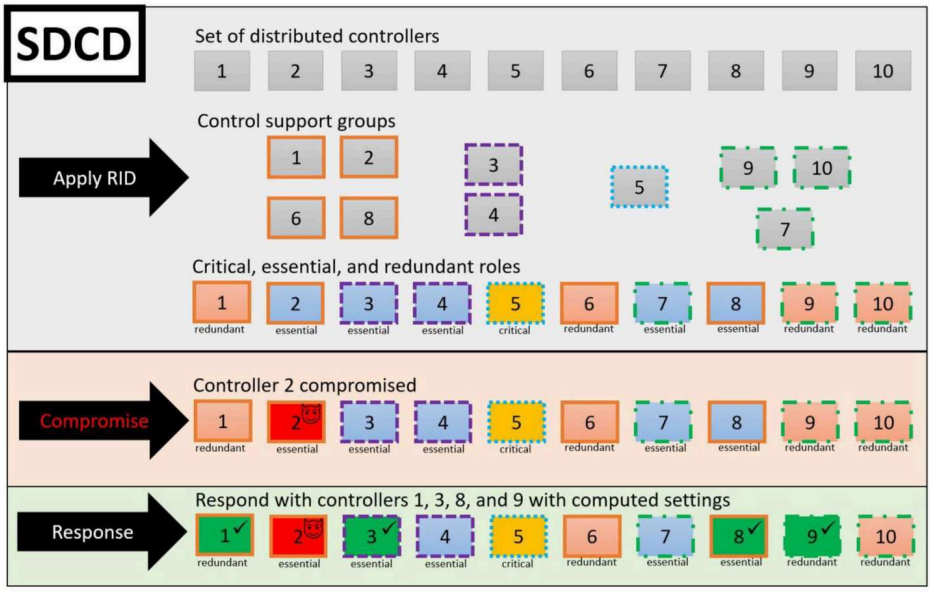

FIGURE 2 Application of SDCD with an example set of 10 distributed controllers; RID computes the control support groups and roles of the controllers. When compromise occurs, the residual, functional set, and RID results are applied to determine which controllers to respond with and using what settings. In this case, controllers 1, 3, 8, and 9 are selected for response

overloads as well as prevention of necessary relay tripping. If unmitigated, these scenarios can lead to equipment damage and/or blackout. While coordinated compromise could potentially cripple the system, whether and how this is possible depends on the specific power system, including its topology and state. Intentional and effective use of controllers in these situations is critical. For example, dynamic reactive support is known to make a difference between an operational system and a blackout [12, 13], and compromise of a certain powerful controllers such as a static var compensator (SVC) can destabilise system voltage [14]. SDCD is a proactive defence against controller compromise that works by identifying and reconfiguring the operating points of select functional controllers in the system based on the system's unique sensitivities and control theory concepts.

2.2 | Offline defence

In the absence of an attack, SDCD is an offline *planning mode* tool for stakeholders to study the amount of flexibility and redundancy provided by available controls for any network and controller configuration. This analysis should begin before an attack occurs because SDCD will reveal control weak points that can inform how to allocate new controllers and measurement devices. The offline, planning stage is a critical time to develop and evaluate online control algorithms that will address natural failures and combat cyber attacks while maintaining operational requirements.

2.3 | Online defence

During or after a compromise, SDCD defends the system under attack by using its framework of controller roles and groups to rapidly determine as well as implement the most effective use of the system's remaining control capabilities. In a distrusted control scenario, the remaining set of controllers needs to quickly respond to ensure that operational reliability (with no violation of limits [15]) is maintained. Additionally, the controller roles and groups can be recomputed with real-time sensitivities to reflect actual system conditions for adaptive control scenarios.

The framework is flexible in that it supports customisable intrusion detection/recovery and stability control strategy mechanisms. During its implementation, appropriate stability control strategies must be deployed, either intrinsically or via an outer control loop as shown in Figure 1. The stability of the power system must be assessed both after compromise or failure and during control response by the distributed controllers. If the system approaches instability, appropriate stability control strategies must be deployed. Such strategies are beyond the scope of this work but can be used in conjunction with the overall framework, as will be discussed in later sections.

2.4 | Related work

The distributed controller RID algorithm that we introduced in [10] identifies the role of each controller, partitioning controller devices into sets that are either critical, essential, or redundant for control of the system, and the control support groups that indicate which controllers are most effective in obtaining some control objective together are obtained.

In contrast to existing literature that mostly focuses on overall system controllability measures [16–19], our work provides individual controller roles as well as the formalisation and application of their interactions for system

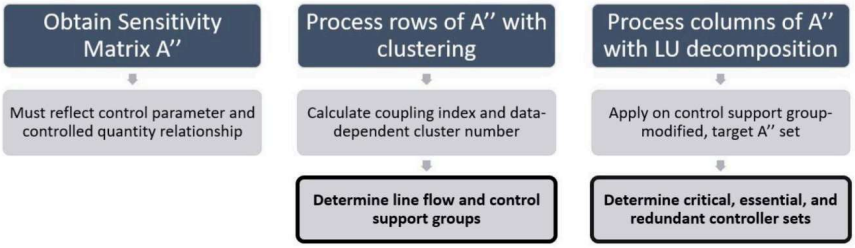

FIGURE 3 Controller role and interaction discovery (RID) method [10] applies clustering and factorisation to categorise controller sensitivities

controllability. SDCD provides an analytical foundation for how to restore or maintain system control under controller attacks using these relationships. Additional review on power system controllability analysis is provided in [20]. This paper presents an innovative approach using control support groups and controller roles for planning and response as part of an overall framework for distributed controller defence.

3 | SDCD: DISTRIBUTED CONTROLLER ROLE AND INTERACTION DISCOVERY

The distributed controller RID algorithm presented in [10] and summarised in Figure 3, identifies essential, critical, and redundant controllers for controllability of the system and identifies control support and line flow groups by processing sensitivity matrices:

- *Essential controllers* are a minimal set of devices required to maintain system controllability; all devices that occur in a minimal-cut set for system controllability are considered essential controllers.
- *Critical controllers* are essential controllers that are irreplaceable and mandatory for system controllability, that is, critical controllers are essential controllers that occur in every minimal-cut controllability set of the system.
- *Redundant controllers* are the devices that reinforce the control capability of essential controllers and can be removed without affecting system controllability.
- *Control support groups* contain devices that are highly coupled in terms of impact on the control objective and with each other.
- *Line flow groups* contain sets of transmission lines where flows in each group can be controlled independently with respect to flows in other groups.

Sensitivity matrices are derived from the nonlinear system model and then utilised to conduct the controllability analysis that identifies the aforementioned roles and groups.

3.1 | Obtaining sensitivity matrix A″

A system's sensitivity matrix $\mathbf{A}''$ is used for control design and stability analysis [21]; contents depend on the control objective. The methodologies developed in this paper are generic in nature and can be suitably applied to any dynamic control support device in the grid. In [10], distributed flexible AC transmission system (D-FACTS) devices are used as the example distributed controllers. We will use this example in this paper for continuity but it is important to note that the RID and SDCD methods can be applied to any distributed controller; the main impact is the construction of the sensitivity matrix.

D-FACTS are currently deployed by SmartWires Inc. [22, 23] in five continents to support grid operation. They include distributed series reactors (DSRs) and distributed static series compensators (DSSCs). Each DSSC acts as a synchronous voltage source in series with the line, changing the line's effective impedance and thus its power flow [22, 24, 25]. The D-FACTS scenarios use total power flow to impedance sensitivities based on the AC power flow equations, topology, and state. The sensitivities are computed analytically as detailed in [26] and reflect both direct (i.e. change in impedance of a line and its direct impact on that line's power flow) and indirect (i.e. change in impedance of a line and its indirect impact on alright other lines' power flows) sensitivities. The sensitivity matrix $\mathbf{A}''$ is found from $\mathbf{\Omega}$,

$$\Delta \mathbf{P}_{flow} = [\mathbf{\Omega}] \cdot \Delta \mathbf{x} \tag{1}$$

where $\Delta \mathbf{P}_{flow}$ are the changes in the line power flows and $\Delta \boldsymbol{x}$ are the impedances. These matrices can be calculated efficiently even for large systems.

3.2 | Finding controllability-equivalence sets

The *line flow groups*, which are of specific interest for D-FACTS devices that are performing power flow control, are found by clustering the sensitivity matrix rows to reveal how lines are affected by each other. Cosine similarity between row vectors $\mathbf{v_i}$ and $\mathbf{v_j}$ of A″ or coupling index **CI** (2) is used to find coupled sets of lines as clusters that are approximately orthogonal to each other [27].

$$\mathbf{CI} = cos(\theta_{\mathbf{v_i v_j}}) = \frac{\mathbf{v_i} \cdot \mathbf{v_j}}{\|\mathbf{v_i}\| \|\mathbf{v_j}\|} \tag{2}$$

Within each group, it is only necessary to control one line flow (the *target lines*) because controlling one such flow impacts the others in a predictable way. $\mathbf{A}''$ is reduced to include

only these target lines. SDCD also identifies how the controllers are related to each other by finding the *control support groups* [28]. These controllability-equivalence sets are determined through clustering using the CI. A well-known challenge for clustering algorithms (e.g. k-means or k-mediods) is the selection of the number of clusters k [29, 30]; therefore, hierarchical agglomerative clustering is chosen as it groups data by creating a cluster tree or dendogram. This is elaborated upon in [10]. The line flows within a cluster are decoupled from flows in other clusters. Flows within a cluster are coupled and mutually dependent.

3.3 | Finding critical, essential, and redundant sets

The *critical*, *essential*, or *redundant* status of a controller is determined based on the coupling of the columns of $\mathbf{A}''$ (rows of $\left[\mathbf{A}''\right]^T$). Essential controllers are linearly independent and have the best control range/influence to meet the objective. While some essential controllers are exchangeable with redundant controllers, other essential controllers are critical controllers that lack redundancy. Particularly, Chen et al. [31] defined a critical measurement as a measurement whose elimination from the measurement set results in an unobservable system. A similar approach is applied to identify critical controllers. lower-upper (LU) factorisation is applied on $\left[\mathbf{A}''\right]^T$ to obtain the change of basis, decomposing the transposed sensitivity matrix to lower and upper triangular factors [32]. The following decomposition of $\left[\mathbf{A}''\right]^T$ is obtained:

$$[\mathbf{A}'']^T = \mathbf{P}^{-1}\mathbf{L_F}\mathbf{U_b} \tag{3}$$

$$\mathbf{L_F} = \begin{bmatrix} \mathbf{L_b} \\ \mathbf{M} \end{bmatrix} \tag{4}$$

Using the Peters–Wilkinson method [32], $\left[\mathbf{A}''\right]^T$ is decomposed (Equation 3); $\mathbf{P}$ is the permutation matrix and $\mathbf{L_b}$ and $\mathbf{U_b}$ are the lower and upper triangular factors of dimension n, respectively. M is a sparse, rectangular matrix with rows corresponding to redundant controllers. The new basis has the structure:

$$\mathbf{L_{CER}} = \mathbf{L}_\beta^{\mathrm{T}} = \mathbf{L_F}\mathbf{L_b^{-1}} = \begin{bmatrix} \mathbf{I_n} \\ \mathbf{R} \end{bmatrix} \tag{5}$$

The new basis, shown in (5), 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. Since, $\mathbf{L_b}$ and $\mathbf{U_b}$ will be non-singular for a controllable system, the rank of $\left[\mathbf{A}''\right]^T$ can be confirmed by checking the rank of the transformed factor $\mathbf{L_F^T}$. Also, $\mathbf{L_b}$ has full rank and with (5) multiplied by $\mathbf{L_b^{-1}}$ from the right, the row identities will be preserved in the transformed matrix $\mathbf{L_F^T}$. Each row of the matrix will, therefore, correspond to the respective controllers [31].

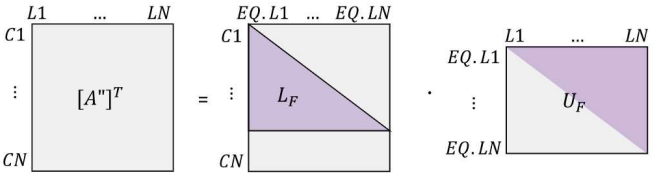

FIGURE 4 Visual representation of LU factorisation of transposed sensitivity matrix where **U** maps the original line flows to equivalent line flows in the transformed basis

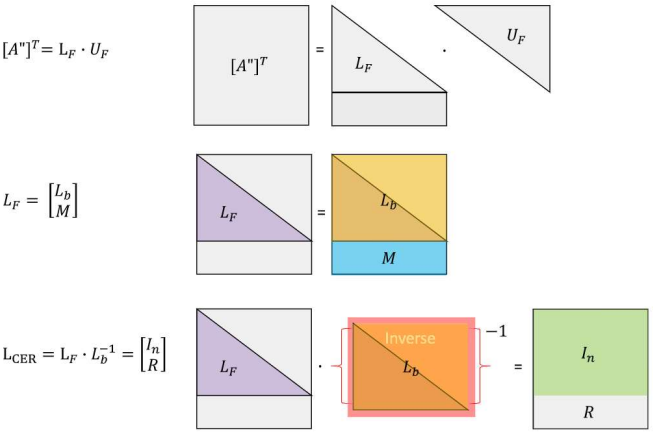

FIGURE 5 The LU factorisation of the transposed sensitivity matrix is illustrated, ultimately resulting in the transformed basis

Rows of $\mathbf{I_n}$ correspond to essential controls that are sufficient to assure independent controllability of the equivalent line flows. Non-zero entries in the rows of $\mathbf{R}$ correspond to redundant controls. Columns correspond to the equivalent flows which can easily be mapped back to the original flows using the permutation matrix $\mathbf{P}$ obtained from the LU decomposition step. The LU decomposition approach preserves and applies the control theory principles that the matrices must have full rank to be controllable/observable.

4 | SDCD FOR OFFLINE CONTROLLER DEFENCE

4.1 | Mapping equivalent line flows

The equivalent line flows are a linear mapping of actual line flows, visualised in Figure 4, and the actual system values can be obtained by traditional back-substitution solution techniques. Thus, the equivalent line flows provide insight into how actual line flows are distributed within the equivalence to better understand how the controller roles are computed. The formulation of the transformed sensitivity matrix $\boldsymbol{L_{CER}}$ is visualised in Figure 5.

Next, to assess the composition of the equivalent line flows, a 7-bus system with D-FACTS devices on all lines is considered [28]; the transformed basis of this system is shown in Figure 6. The remainder of this section demonstrates the implementation of the RID methodology for this 7-bus

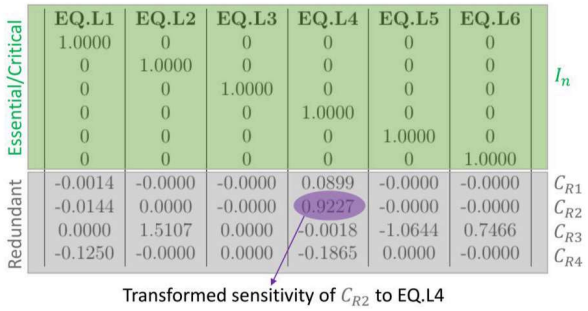

FIGURE 6 Transformed basis L_{CER} with labelled controller roles for 7-bus system

system. The 7-bus system is a demonstrative case from the Glover et al. textbook, as well as a PowerWorld Simulator public test case [33]. The 7-bus system is used as a simple case-study in presenting the SDCD strategy in an understandable way. Results from the SDCD method will also be demonstrated with the same 7-bus system in Section 7.

Using the analysis techniques described above, the transformed basis $\boldsymbol{L_{CER}}$ is obtained for the 7-bus system as shown in Figure 6. An example result from the transformed basis, highlighted in purple in Figure 6, shows that by studying the transformed sensitivity of the redundant controller C_{R2} to the equivalent line flow 4, one can easily map back to obtain the original line flow composition of **EQ.L4**.

The entries in $\mathbf{U_F}$ (Figure 5) are weightings of the original line flows in the equivalent line flows. $\mathbf{U_F}$ for the 7-bus system is shown in Table 1, where its entries determine the composition of the equivalent line flows as linear combinations of the original target line flows T_j, where j is the index over alright target lines, as shown in Equations (6)–(12). The target line flow, T_j is defined for the purposes of this analysis as the real power flow of the target set of transmission lines that can be independently controlled.

$$\begin{aligned}\textbf{EQ.L1} = {} & 1.9165 \cdot T_1 - 0.3014 \cdot T_2 + 0.6138 \cdot T_3 \\ & + 0.4783 \cdot T_4 - 0.7696 \cdot T_5 + 1.3766 \cdot T_6 \end{aligned} \tag{6}$$

$$\begin{aligned}\textbf{EQ.L2} = {} & -1.6761 \cdot T_2 - 0.5473 \cdot T_3 - 0.7116 \cdot T_4 \\ & - 0.9459 \cdot T_5 + 0.4046 \cdot T_6 \end{aligned} \tag{7}$$

$$\textbf{EQ.L3} = -1.4221 \cdot T_3 + 0.7592 \cdot T_4 - 0.7507 \cdot T_5 \tag{8}$$

$$-0.6497 \cdot T_6 \tag{9}$$

$$\textbf{EQ.L4} = 1.2547 \cdot T_4 - 1.2407 \cdot T_5 + 1.2444 \cdot T_6 \tag{10}$$

$$\textbf{EQ.L5} = -0.0041 \cdot T_5 + 0.0113 \cdot T_6 \tag{11}$$

$$\textbf{EQ.L6} = -0.0063 \cdot T_6 \tag{12}$$

Equations (6)–(12) indicate the linear mapping between the target line flows and the equivalent line flows. The equivalent line **EQ.Li** flows are expressed in terms of the target line flows T_j to identify the sets of redundant and non-redundant control devices.

TABLE 1 The upper triangular factor matrix $\mathbf{U_F}$ of the 7-bus system's sensitivity matrix provides weightings between equivalent (transformed)line flows **EQ.Li** and original flows T_j

	T1	T2	T3	T4	T5	T6
EQ.L1	1.9165	−0.3014	0.6138	0.4783	−0.7696	1.3766
EQ.L2	0	−1.6761	−0.5473	−0.7116	−0.9459	0.4046
EQ.L3	0	0	−1.4221	0.7592	−0.7507	−0.6497
EQ.L4	0	0	0	1.2547	−1.2407	1.2444
EQ.L5	0	0	0	0	−0.0041	0.0113
EQ.L6	0	0	0	0	0	−0.0063

TABLE 2 Ranking of controller groups in descending order of the effectiveness using equivalent line flows for the 7-bus system

Ranking of redundant controllers		
Equivalent line	**Effective controllers**	**Ineffective controllers**
EQ.L1	$C_{R4} > C_{R3} > C_{R2}$	C_{R3}
EQ.L2	C_{R3}	C_{R1}, C_{R2}, C_{R4}
EQ.L3	N/A	C_{R1}, C_{R2}, C_{R3}, C_{R4}
EQ.L4	$C_{R2} > C_{R4} > C_{R1} > C_{R3}$	N/A
EQ.L5	C_{R3}	C_{R1}, C_{R2}, C_{R4}
EQ.L6	C_{R3}	C_{R1}, C_{R2}, C_{R4}

4.2 | Ranking redundant controllers

The transformed basis in Figure 6 also reveals how the redundant controllers labelled $C_{R1} - C_{R4}$ should be ranked. When compromise or failure occurs for any essential controllers (in $\mathbf{I_n}$), the redundant controllers should respond. The entries of $\mathbf{R}$ give the sensitivity of each equivalent line flow to each redundant controller.

If the essential controller of **EQ.L4** is compromised, from the transformed basis it is clear that redundant controller C_{R2} has the highest impact on **EQ.L4** and is thus of the highest importance for responding to that compromise. C_{R4} has the next highest sensitivity and can be used in conjunction with or subsequent to C_{R2}. Both C_{R1} and C_{R3} have low sensitivities and would not be effective if used alone. Based on the specific compromise or failure situation, these rankings can be used to employ the most sensitive redundant controllers or utilise all controllers such that highly ranked controllers are prioritised. Table 2 summarises the ranking of the redundant controllers for the six equivalent line flows computed for a selected operating point of the system.

4.3 | Improving controller placement

When no other controller can provide needed control of the corresponding equivalent line flow (i.e. *Critical Controller*), the decomposition reveals where to add a redundant controller.

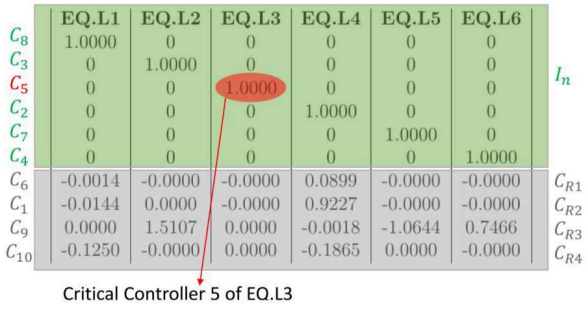

FIGURE 7 Transformed basis L_{CER} with labelled critical controller for 7-bus system. The grey rows correspond to redundant controllers, and a controller is considered critical if its corresponding equivalent line flow is unity when all other elements in that column is zero

Relevant techniques have been developed for phasor measurement unit (PMU) placement and observability, and these can be extended to controllers [34]. In the 7-bus example, Controller 5 corresponding to **EQ.L3** of the transformed basis is critical, as shown in Figure 7. The composition of $EQ.L3$ is shown in (9), where T_3 provides the most significant contribution to **EQ.L3**. The target line selections are T_j, and the mapping to the actual line indices in the 7-bus system is the following: T_1: L_1, T_2: L_3, T_3: L_5, T_4: L_7, T_5: L_9, and T_6: L_{10}. That is, T_3 corresponds to L_5 in the 7-bus system, and is based on the selection of target line flows. After another controller is added to be redundant to Line 5, the transformed basis after re-factorising the matrix is obtained (Table 3).

Controller 6 shown in Figure 8 is redundant to **EQ.L3** and converts controller 5 from critical to essential—with magnitude 1 in the transformed basis, Controllers 5 and 6 are now interchangeable for controlling **EQ.L3**. By eliminating critical controllers, the risk of loss of system controllability is now reduced.

This type of study can be performed as a planning tool for placing distributed controllers such that there exist no critical controllers, while unnecessary controllers are avoided. The compositions of the equivalent line flows in terms of the original line flows aid controller placement to avoid critical roles and eliminate excessive redundancy. Rankings of redundant controllers from the transformed sensitivities during essential controller compromise or failure can be used to give the most effective redundant controllers and to avoid using controllers that have little or no impact.

5 | SDCD: RESPONDING TO CONTROLLER COMPROMISE

Once compromise of a distributed controller is detected, that is, by an intrusion detection system (IDS) or basic detection of rapid or unnecessary controller settings changes, the optimal response process can be deployed with the remaining distributed controllers.

In systems without IDS or the security features needed to identify a compromised controller, a deteriorating system state may be the only indication of abnormal behaviour. In these cases, physical controls can respond immediately while cyber-side abnormalities are investigated and repaired. It should be noted that control support group responses cannot always completely mitigate the effects of *distrusted controllers*. In some cases, there may simply be no support group for the affected lines. In other cases, the control support groups might not be able to manipulate the power flow in their lines sufficiently to offset the undesired system behaviour. These circumstances can be averted in the offline planning stage (Section 4) through careful attention to optimal controller placement and redundancies.

TABLE 3 Transformed basis with added redundant controller to line 5

EQ.L1	EQ.L2	EQ.L3	EQ.L4	EQ.L5	EQ.L6
1.0000	0	0	0	0	0
0	1.0000	0	0	0	0
0	0	1.0000	0	0	0
0	0	0	1.0000	0	0
0	0	0	0	1.0000	0
0	0	0	0	0	1.0000
−0.0014	−0.0000	−0.0000	0.0899	−0.0000	−0.0000
−0.0000	0.0000	1.0000	−0.0000	−0.0000	0.0000
−0.0144	0.0000	−0.0000	0.9227	−0.0000	−0.0000
0.0000	1.5107	0.0000	−0.0018	−1.0644	0.7466
−0.1250	−0.0000	0.0000	−0.1865	0.0000	−0.0000

When the compromise of any distributed controller occurs, the appropriate response of the remaining controllers must be formulated, using the SDCD algorithm, to minimise stressed conditions and prevent damage to sensitive equipment. *Recurrent sets* (sets of controllers that frequently occur together in transformed sensitivity analyses taken over time), can be used to select controllers that maximise controllability across a range of operating points. An optimisation framework and control algorithm is applied, using the generic objective function f_0 in Equation (13) to minimise the differences between the actual and desired quantities,

$$f_0 = \sum_{i=1}^{N} [P_{flow,desired}(x) - P_{flow,actual}(x)]_i^2 \quad (13)$$

$$min\ f_0 \quad (14)$$

$$s.t.\ \mathbf{f}_{(p,q)}(\mathbf{s}_{(\theta,V)}) = 0 \quad (15)$$

$$\mathbf{x} \leq \mathbf{x}_{max} \quad (16)$$

$$\mathbf{x} \geq \mathbf{x}_{min} \quad (17)$$

where N represents the number of lines to be targeted for control. The constraints are AC power balance and device limits. The formulation is solved using the reduced gradient method and described in more detail in [28].

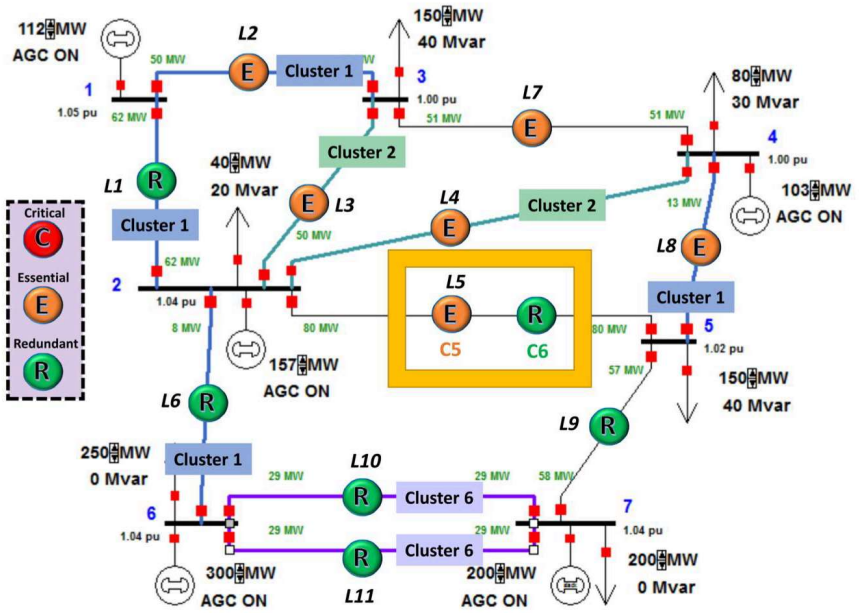

FIGURE 8 The 7-bus system with lines coloured according to cluster group and labelled with essential and redundant controllers. Highlighted in the yellow box is added controller C6 which converts C5 from critical to essential

6 | STATE DEPENDENCE OF ROLES AND GROUPS

The previous sections discuss the insights gained from the transformed sensitivity matrix basis and show how that information can be leveraged. In order for control systems to take advantage of these results, it is necessary to examine the extent to which the controller roles and control support groups change with varying operating states of the power system. The 7-bus system was studied with different settings of the D-FACTS controllers. The effective impedance of each device, was varied to ±30% of the line impedance where the ±30% variation is based on the real-world D-FACTS device limits [35]. In the 7-bus system, 10 lines have D-FACTS devices, and each is given one of three different settings [$x_{DF,LOW}$ $x_{DF,0}$ $x_{DF,HIGH}$], where $x_{DF,0}$ indicates the controller is not in use and the line is at its original impedance.

The first scenario uses two D-FACTS at a time and considers 900 setting states. The second scenario uses combinations of four controllers in the same manner, resulting in 81,000 setting states. Four device combinations are the maximum considered for this study due to the computational burden. With these operating points and device combinations, controller role and control support groups are recalculated and compared. Figure 9, in the labelled #1 and #2 plots, shows the number of occurrences (*y*-axis) of each controller (*x*-axis) as essential or critical over all the operating points. Results indicate that a pattern of *recurrent essential controllers* and *recurrent critical controllers* emerges. Controllers 1, 2, 3, 8, 9 frequently appear as essential over all the operating points. Similarly, plots #3 and #4 of Figure 9 show the number of occurrences for each controller as critical over all operating points, for both two and four device combinations.

These results highlight two main points: (1) the controller roles can change as the operating point varies; and (2) some controllers frequently appear in a certain role. Then, to further explore these observations, the effective impedance of each device was varied ±90% of the line impedance to study dramatically different operating points.

For two D-FACTS combinations, a pattern broadly emerges, with Controllers 8, 9 increasing in frequency for critical role assignment.

For four D-FACTS combinations, the results have higher variation. Controllers 1, 2, 3, 8, 9 retain high frequency as essential or critical and Controller 5 retains the highest number of occurrences as critical. However, Controllers 4, 6, 8, 9 exhibit higher numbers of occurrences as critical. This provides the insight that it may be necessary to factor in the operating point of the system during remedial actions.

Cluster membership in control support groups was also tracked in the above experiments to measure how frequently the controllers changed clusters, with the results summarised in Figure 10.

The IEEE 118-bus system was tested using this procedure with varying operating points, for both ±30% and ±90% changes in x_{LINE}. D-FACTS were presumed to be on every line (186 lines) and a change in a single device was considered at a time. As the operating point changes, the resultant controller roles remain the same for both ±30% and ±90% changes. More significant changes such as line outages and faults may impact the groups, even in a large system. When recurrent sets of controller roles exist, they can be used to aid a priori response calculations. In the 118-bus system, the analysis showed that of the 186 lines in the system, none were *critical*, while 96 were found to be *essential*, and 90 were found to be *redundant* to system controllability, with 91 control support groups for the system.

The main observations from studying cluster membership over different operating points are the following:

(1) For the different scenarios of D-FACTS combination cases, the results are similar and show distinct cluster membership.

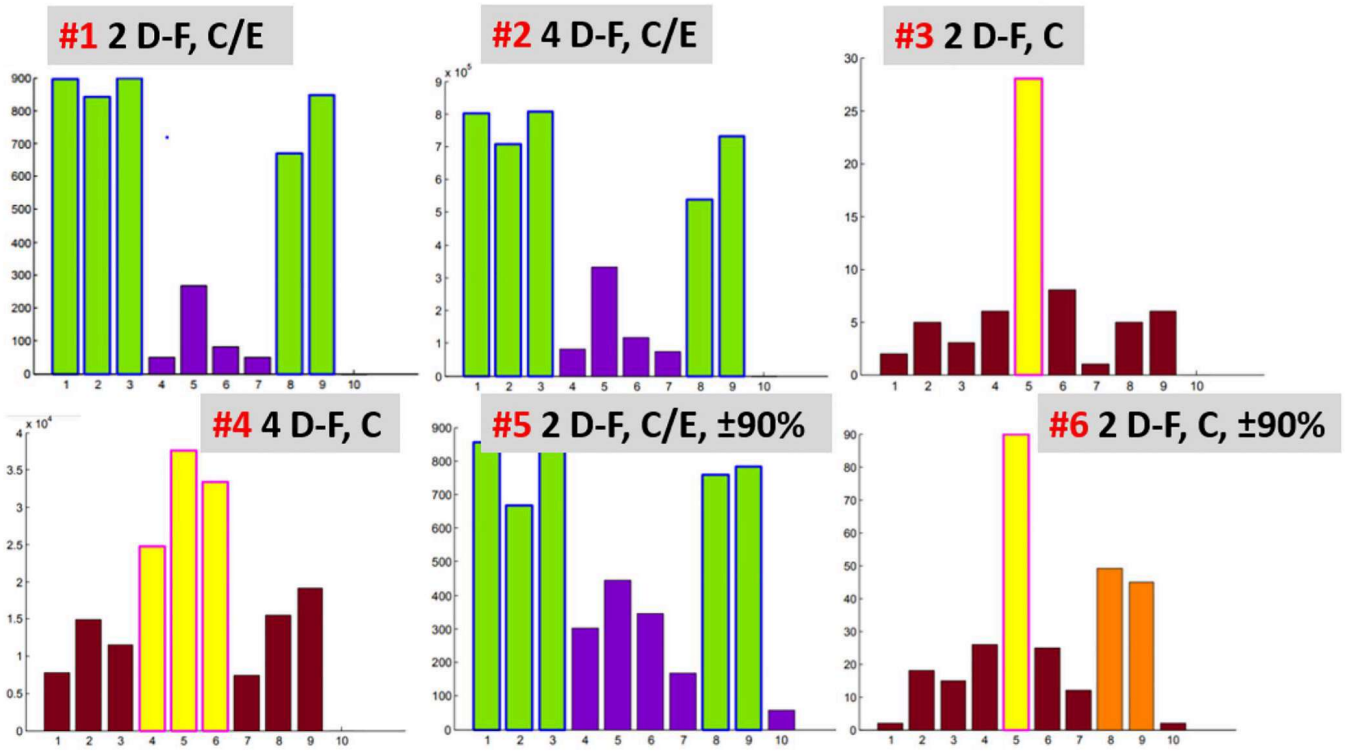

FIGURE 9 Occurrences of each controller as critical/essential (C/E) or just critical (C) overall operating points for different number of D-FACTS combinations (2 or 4 D-F). Results for line impedance, x_{LINE}, variation of ±90% is also shown in plots #5 and #6. The controller # is on the *x*-axis and the number of occurrences is on the *y*-axis

(2) For large variations in line impedances, cluster membership patterns become less distinct, though the same controllers still appear dominant.

(3) For small changes in larger systems, controller roles often stay the same.

These frequencies of occurrences and operation points of the controllers are used to develop various controller selection techniques for mitigation. Namely, the *Recurrent CE* and *Recurrent R* selection methods use controller roles with the highest frequency of occurrence (over the operating points), for critical/essential roles and redundant roles, respectively. These selection techniques factor in sensitivity computations made over various operating points of the system to form control support groups. The *Current CE*, *Current R*, and *Ranked R* selection methods are calculated with the current operating point of the system. These selection methods and their impact in mitigating controller compromise is demonstrated in the next section for both the 7-bus and IEEE 118-bus systems using the SDCD approach.

7 | RESULTS AND DISCUSSION

The selection algorithms discussed above were implemented for two test cases; the 7-bus system detailed in previous sections, and the IEEE 118-bus system. SDCD results use power system metrics to measure performance and to optimise response using distributed controllers. The megavolt-ampere (MVA), a measure of apparent power, percentage loading of lines is used as a metric for power system tolerance. The MVA limits of lines are a common indicator of physical power system impact, for example, in optimal power flow formulations. Other performance metrics may also be applied when implementing SDCD, where the equations used in the algorithm would be modified accordingly. Calculating response and measuring performance with these metrics, cyber-physical intrusion tolerance of the power system is improved by minimising the impact of a compromise or intrusion with the deployment of coordinated controls.

7.1 | 7-bus system

While the use of 10 controllers could be considered superfluous for this system, it is designed to illustrate the possibilities of various support groups that can be used to mitigate controller compromise and to highlight controller locations that cannot be mitigated using support group selections.

In the 7-bus system, Controller #2 was compromised, with the compromise causing an increase in Line 2 power flow. Table 4 presents the results. The compromised controller is mitigated through the various selection methods, and for this scenario, the effectiveness of the algorithms is based on the % MVA flows for all lines in the system.Based on this metric, the best performing selection scheme was found to be *Recurrent CE*, while *Current R* selection

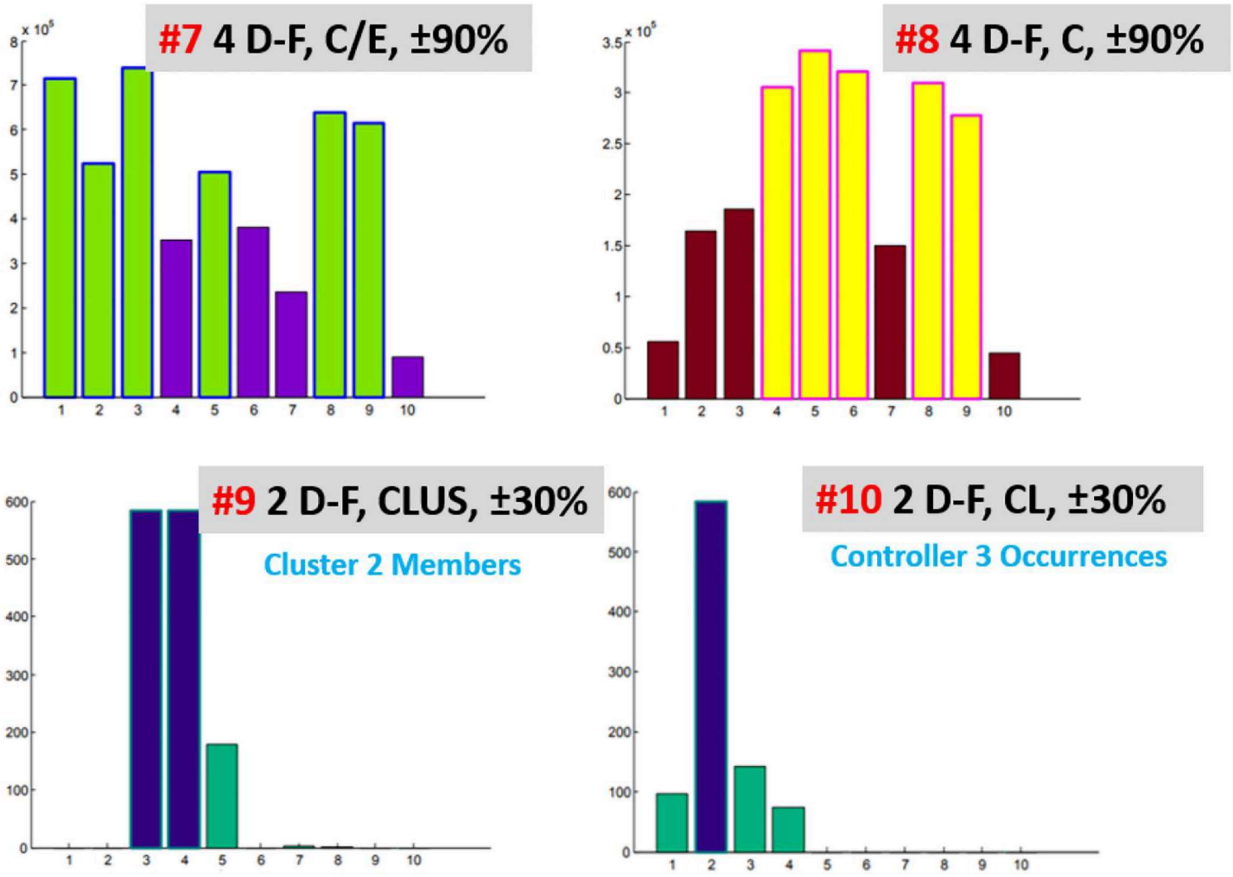

FIGURE 10 Results for line impedance, x_{LINE}, variation of ±90% are shown in plots #7 and #8. The *x*-axis represents the controller # and the *y*-axis provides the number of occurrences. Plot #9, with the same labelled axes, provides the frequency of each controller in Cluster 2. Plot #10 shows the frequency of Controller 3 being assigned to every cluster with Cluster # on the *x*-axis and number of occurrences on the *y*-axis. Both cluster plots consider a ±30% change in x_{LINE}

TABLE 4 Responding to Controller 2 compromise with various response controllers (C#) at high load in the 7-bus system; Original MVA_{L2} = 89%. Mean line flow is used as a metric as the original system (before compromise) was structured to have similar line flows on all other lines

Controller #2 Compromise (original line flow: 89% MVA_{L2})			
Selection method	**Response C #**	**MVA_{L2}**	**Mean system MVA**
Recurrent CE	1,3,8,9	79.6%	53.0%
Recurrent R	4,5,6,7,10	61.1%	56.4%
Current CE	3,4,5,6,7	76.7%	55.4%
Current R	1,3,7	76.6%	58.2%
Current ranked R	1,3,10	79.9%	56.1%

provided the least effective results under this scenario. While the *Current CE* and *Current R* techniques (that factor in the present operating point) provide a better reduction of power-flow in Line 2 (the compromised line), when the measure of effectiveness is changed to the mean system MVA, selection techniques that depend primarily on the system topology perform better.

Table 5 presents the results for various compromised controller scenarios using only the *Recurrent CE* controller set, where original, compromised, and response % MVA is given for each targeted line. The settings for the response set $\mathbf{C}_{\#_{Resp.}}$, which excludes compromised controllers, are computed using Equations (13)–(17). In most cases, the response set is able to significantly reduce the line flow % MVA.

These results indicate that the SDCD algorithm's flexibility is effective in either restoring a system's overall line flows to the original state before a compromise, or restoring that of a particular line solely. Depending on the objective, an appropriate selection technique can be used.

7.2 | IEEE 118-bus system

The methodology was also tested on the larger IEEE 118-bus system shown in Figure 11. In this system, the controller on Line 63 (illustrated in orange in Figure 11 is selected as the compromised controller, with Controllers # 50, 68, 69, and 117 selected using the *Recurrent R* method, acting as the support groups, highlighted in blue in Figure 11.

Under the selected scenario, at the current system operating point, Line 63 had a power flow at 80.4% of line capacity. The compromise of the controller pushes up the power flow to 94.76% of line capacity. Following the recalculation of settings of

TABLE 5 Responding to controller compromises with recurrent CE response set and calculated settings

$C\#_{Compr.}$	x_{DF} (*pu*)	MVA $_{L\#,Orig.}$	MVA $_{L\#,Compr.}$	$C\#_{Resp.}$	Settings (*pu*)	MVA $_{L\#,Resp.}$
4	−0.054	44.5%	56.8%	1,2,3,8,9	0.015, −0.072, −0.054, 0.072, −0.018	46.8%
5	−0.036	67.6%	78.6%	1,2,3,8,9	0.015, −0.072, −0.054, −0.072, −0.018	71.9%
7	−0.009	23.5%	24.3%	1,2,3,8,9	0.0088, −0.0077, −0.0127, 0.002, 0.0017	22.9%
10	−0.072	14%	17.6%	1,2,3,8,9	0.015, −0.072, −0.054, −0.072, 0.018	15.7%
2,10	−0.072, −0.072	44.2%, 14%	55.5%, 17.3%	1,3,8,9	−0.015, −0.054, 0.072, 0.018	49%, 16.3%
4,5,9	−0.054, −0.036, −0.018	44.5%, 67.6%, 32.8%	53.8%, 74.4%, 31.5%	1,2,3,8	0.015, −0.072, −0.054, −0.072	46.8%, 70.4%, 31.6%

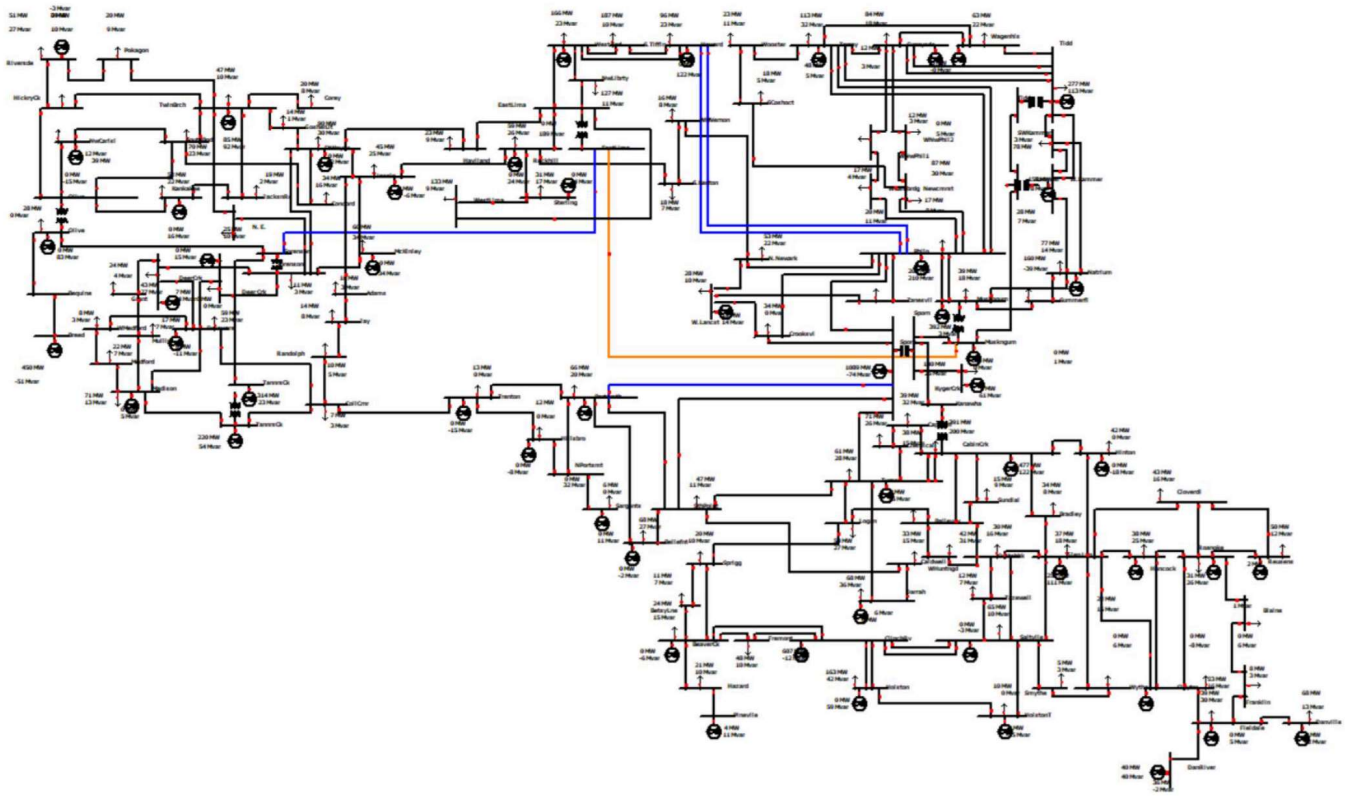

FIGURE 11 IEEE 118-bus System used for testing, with the compromised line highlighted in orange and support group lines highlighted in blue

the other controllers, the power flow improves to 84.6% of the limit. The results of the line flows are summarised in Table 6.

It is observed that the failure of the controller on Line 63 increased the overall real power transmission loss by 4.03% and the reactive power transmission loss by 57.71%. After the recalculation of settings of the other controllers, the real power transmission loss did not improve greatly. However, the reactive power transmission loss improved by 11% over the operating state of the system during failure, with the post-mitigation loss being a significantly lower 40.6% decrease over the pre-failure operating state of the system. These results are presented in Table 7.

TABLE 6 Summary of the % MVA flows in the target lines during failure and post-correction for the IEEE 118-bus system

Controller #63 compromise (original: 84.76% MVA_{L63})		
Line #	**% MVA during failure**	**% MVA post-correction**
63	94.76%	84.6%
50	21.55%	28.32%
68	36.75%	41.25%
69	36.75%	41.25%
117	63.58%	75.71%

TABLE 7 Summary of the real and reactive power flow losses in the IEEE118-bus system for a single controller attack scenario with the objective to reduce target line's flow

Controller #63 compromise (original: 84.76% MVA_{L63})				
Scenario	**Real power loss (MW)**	**Reactive power loss (MVAr)**	**% increase in real power loss**	**% increase in reactive power loss**
Before failure	257.87	137.11	N/A	N/A
During failure	268.08	216.54	4.03%	57.713%
Post correction	268.25	192.84	4.09%	40.6%

TABLE 8 Comparison of the effectiveness of selection techniques (S. No) for the IEEE 118-bus system. It is observed that considerable improvement in losses are obtained even with redundant (less effective) controllers

S. No	Mitigation selection technique	Losses
-	Normal operation	264.471 MW, 181.327 MVAR
-	Coordinated attack scenario	268.076 MW, 216.541 MVAR
1	Recurrent R	268.024 MW, 202.711 MVAR
2	Recurrent CE	268.917 MW, 187.337 MVAR
3	Current ranked R	266.258 MW, 200.315 MVAR

The results for the IEEE 118-bus system provide multiple key insights:

(1) Results reiterate observations from the 7-bus system that the line clusters and support groups do not need to be localised, and they are highly dependent on system topology as well as the distribution of loads and generators across the system.

(2) Results indicate how to utilise knowledge of the system to generate remedial schemes that ensure grid operation without limit violations using distributed controllers in the system rather than merely using localised elements/devices in the immediate neighbourhood.

Following the single attack cases, the SDCD strategy is also tested for a scenario of coordinated attack, where several essential controllers on Lines 14, 63, 81, and 117 are compromised. The aim of this attack is to reduce power flow on lines with high capacity and force it to be routed through lines with low capacity. The SDCD recomputes settings of controllers in other high capacity lines to mitigate this event. In this scenario, the high capacity lines have functional D-FACTS devices that enable higher power flow. When these devices are compromised, they can reduce the overall system efficiency by manipulating the effective impedance of the lines with compromised D-FACTS devices and, consequently, cause line overloading.

Under this scenario, other controllers in the concerned support groups are selected and their settings are reconfigured to redirect power flow through them and improve system efficiency while reducing the loading on lines that were affected by the attack. Table 8 provides data pertaining to overall system efficiency that indicates how SDCD strategy can be used to move the system closer to its original operational state during times of an attack, with the metric of system losses being used.

It is pertinent to note from the results that SDCD is effective even in scenarios where *only* controllers with lower impact (*Recurrent R* selection), that is, redundantly ranked devices, are available for mitigation. Additionally, the *Recurrent R* selection controllers are not recalculated using current system state and can be computed offline, in advance. Using more effective techniques such as *Current CE, Recurrent CE* etc. can provide more benefit with current system state, but may not be necessary for all scenarios. Thus, the SDCD approach can be used flexibly for different systems, controller sets, and operational needs. The results of these other selection techniques are compared in Table 8.

8 | CONCLUSION

This paper presents a process to restore control and reliable steady-state operation using the SDCD method, given the compromise or failure of distributed devices on the grid. In summary, the core contributions of this paper are as follows:

(1) Discovering the equivalent sensitivity parameters to identify redundancies by using the transformed basis that is obtained by decomposition and factorisation of desired system sensitivities.

(2) Aiding controller placement to avoid critical roles, avoid excessive redundancy, and rank redundancies based on their effectiveness to the selected parameter.

(3) Exploring system state (operating point) dependence of role and group recurrent behaviour exhibited in the results.

(4) Development of a control response framework for the compromise or failure of distributed device(s) in a system based on a desired objective. This was demonstrated for a 7-bus and the IEEE 118-bus systems with both single controller and coordinated attack.

The response mechanisms highlighted in this paper are designed to be deployed during an incident to reduce system stress and mitigate compromise consequences while the actual cause and removal of the compromise is investigated by intrusion detection and recovery methods, or other security mechanisms.

ACKNOWLEDGMENTS

This work was supported in part by the National Science Foundation (NSF) under Award Numbers CNS 1446229 and CNS 1446471 and the U.S. Department of Energy Cybersecurity for Energy Delivery Systems (CEDS) under Award Number DE-OE0000895.

This paper describes objective technical results and analysis. Any subjective views or opinions that might be expressed in the paper do not necessarily represent the views of the U.S. Department of Energy or the United States Government.

REFERENCES

1. EY's 19th Global Information Security Survey 2016-17: Path to cyber resilience: sense, resist, react (2017). http://www.ey.com/gl/en/industries/power---utilities/ey-the-path-to-cyber-resilience-sense-resist-react#section8 Accessed 01 May 2017
2. Liu, C.-C., et al.: Intruders in the grid. IEEE Power Energy Mag. 10(1), 58–66 (2012)
3. Falliere, N., Murchu, L.O., Chien, E.: W32.Stuxnet dossier. Symantic Security Response (2010)
4. Assante, M.J.: Confirmation of a coordinated attack on the Ukrainian power grid. SANS Industrial Control Systems (2016). ics.sans.org/blog/2016/01/09/confirmation-of-a-coordinated-attack-on-the-ukrainian-power-grid
5. Dragos Security: Crashoverride: analysis of the threat to electric grid operations (2017). https://dragos.com/blog/crashoverride/CrashOverride-01.pdf Accessed 01 May 2017
6. Hayden, E., Assante, M., Conway, T.: An abbreviated history of automation & industrial controls systems and cybersecurity. SANS analyst white papers (2014)
7. Yazdanian, M., Mehrizi-Sani, A.: Distributed control techniques in microgrids. IEEE Trans. Smart Grid. 5(6), 2901–2909 (2014)
8. Aquino-Lugo, A.A., Klump, R., Overbye, T.J.: A control framework for the smart grid for voltage support using agent-based technologies. IEEE Trans. Smart Grid. 2(1), 173–180 (2011)
9. Vedady Moghadam, M.R., Ma, R.T.B., Zhang, R.: Distributed frequency control in smart grids via randomized demand response. IEEE Trans. Smart Grid. 5(6), 2798–2809 (2014)
10. Hossain.McKenzie, S., et al.: Distributed controller role and interaction discovery. In: 2017 19th international conference on intelligent system Application to power systems (ISAP), pp. 1–6. San Antonio, Texas (2017)
11. Hossain.McKenzie, S.S.: Protecting the power grid: strategies against distributed controller compromise. University of Illinois at Urbana-Champaign Urbana, Illinois (2017)
12. Report on the grid disturbances on 30th July and 31st July 2012. Government of India (2012). http://www.cercind.gov.in/2012/orders/Final_Report_Grid_Disturbance.pdf Accessed 01 May 2017
13. Bhattacharya, K., Bollen, M., Daalder, J.E.: Operation of restructured power systems. In: Power Electronics and power systems. Springer US (2001)
14. Chen, B., Butler.Purry, K.L., Kundur, D.: Impact analysis of transient stability due to cyber attack on FACTS devices. In: North American power Symposium (NAPS), 2013, pp. 1–6. Manhattan, Kansas (2013)
15. Liacco, T.E.D.: The adaptive reliability control system. IEEE Trans. Power Apparatus Syst. PAS-86(5), 517–531 (1967)
16. Bobba, R.B., et al.: Detecting false data injection attacks on dc state estimation. In: Preprints of the first workshop on secure control systems, CPSWEEK (2010)
17. Hamdan, A.M.A., Elabdalla, A.M.: Geometric measures of modal controllability and observability of power system models. Elec. Power Syst. Res. 15(2), 147–155 (1988)
18. Hamdan, A.M.A., Nayfeh, A.H.: Measures of modal controllability and observability for first- and second-order linear systems. J. Guid. Contr. Dynam. 12(3), 421–428 (1989)
19. Messina, A., Nayebzadeh, M.: An efficient placement algorithm of multiple controllers for damping power system oscillations. In: Power Engineering Society Summer Meeting, 1999. IEEE, vol. 2, pp. 1280–1285. IEEE, Edmonton, AB, Canada (1999)
20. Hossain McKenzie, S., et al.: Analytic corrective control selection for online remedial action scheme design in a cyber adversarial environment. IET Cyber-Physical Systems: Theory & Applications 2(4), 188–197 (2017)
21. Dahleh, M.A., Diaz.Bobillo, I.J.: Control of Uncertain systems: a linear Programing approach. Prentice Hall (1995)
22. Divan, D.: Improving power line utilization and performance with d-facts devices. In: IEEE Power Engineering Society general meeting, 2005, pp. 2419–2424. IEEE, San Francisco, CA (2005)
23. SmartWireGrid: Minnesota power deploys smart wires to optimise its grid and save customers money (2016). http://www.smartwires.com/category/press-release/ Accessed 01 August 2016
24. Divan, D.M., et al.: A distributed static series compensator system for realizing active power flow control on existing power lines. IEEE Trans. Power Delivery. 22(1), 642–649 (2007)
25. Johal, H., Divan, D.: Design considerations for series-connected distributed FACTS converters. IEEE Trans. Ind. Applicat. 43(6), 1609–1618 (2007)
26. Rogers, K.: Power system control with distributed flexible AC transmission system devices. University of Illinois at Urbana-Champaign (2009)
27. Rogers, K.M. et al.: Smart-grid -enabled load and distributed generation as a reactive resource. In: Innovative smart grid technologies (ISGT), 2010, pp. 1–8 (2010)
28. Rogers, K.M., Overbye, T.J.: Power flow control with distributed flexible ac transmission system (D-FACTS) devices. In: 41st North American power symposium, pp. 1–6. Starkville, Mississippi (2009)
29. Hartigan, J.A., Wong, M.A.: Algorithm as 136: a k-means clustering algorithm. Appl. Stat. 28(1), 100–108 (1979)
30. Park, H.-S., Jun, C.-H.: A simple and fast algorithm for k-medoids clustering. Expert Syst. Appl. 36(2), 3336–3341 (2009)
31. Chen, J., Abur, A.: Placement of PMUs to enable bad data detection in state estimation. IEEE Trans. Power. Syst. 21(4), 1608–1615 (2006)
32. Peters, G., Wilkinson, J.H.: The least squares problem and pseudo-inverses. Comput. J. 13(3), 309–316 (1970)
33. Glover, J.D., Sarma, M., Overbye, T.: Power system Analysis & design, SI Version. Cengage Learning (2011)
34. Chen, J., Abur, A.: Placement of PMUs to enable bad data detection in state estimation. IEEE Trans. Power Syst. 21(4), 1608–1615 (2006)
35. PowerWorld Corporation: D-FACTS quick-start tutorial (2016). http://www.powerworld.com/knowledge-base/d-facts-quick-start-tutorial Accessed 01 January 2017
36. Xu, B., Abur, A.: Observability analysis and measurement placement for systems with pmus. In: Power systems conference and exposition, 2004, vol. 2, pp. 943–946. IEEE PES (2004)
37. Wood, A.J., Wollenberg, B.F.: Power generation, operation, and control. John Wiley & Sons (2012)
38. Sauer, P.W., Pai, M.A., Chow, J.H.: Power system dynamics and stability: with synchrophasor measurement and power system toolbox. IEEE. Wiley (2017)
39. Xiang, Y., et al.: Impact of UPFC on power system reliability considering its cyber vulnerability. In: 2014 IEEE PES T & D conference and exposition, pp. 1–5, Chicago, IL (2014)
40. Ding, T., et al.: Optimal power flow with the consideration of flexible transmission line impedance. IEEE Trans. Power Syst. 31(2), 1655–1656 (2016)

How to cite this article: Hossain-McKenzie S, Raghunath K, Davis K, Etigowni S, Zonouz S. Strategy for distributed controller defence: Leveraging controller roles and control support groups to maintain or regain control in cyber-adversarial power systems. *IET Cyber-Phys. Syst., Theory Appl*. 2021;6;80–92. https://doi.org/10.1049/cps2.12006