Mitigating Against a Succession of Hidden Failure Accelerants Involved in an Insider Threat Sequential Topology Attack on a Smart Grid

Devising a Defensive Paradigm via a Bespoke Convolutional Adversarial Neural Network Module and Particle Swarm Optimization-based Enhanced Reinforcement Learning Component

Steve Chan
Decision Engineering Analysis Laboratory, VTIRL, VT
Orlando, USA
e-mail: schan@dengineering.org

***Abstract*—Protection System Hidden Failures (PSHF)-induced sequential events have been shown to have higher impact and greater likelihood of segueing to major outages. Hence, a pragmatic mitigation approach is to intercede in the outage-related successive event stream. From a cyber perspective, as pertains to the power grid, PSHF are comparable to a Zero-Day attack (a.k.a. "0-Day"); accordingly, adequate mitigation is not yet in place. This problem is particularly interesting because of the involved paradox; although widely accepted to be comparable to a 0-Day, some form of apriori architected mitigation is crucial so as to prevent a major outage. This can be construed as contributory toward resiliency. Accordingly, a pseudo-inverse approach is taken to the optimal controllability problem (in this case, non-optimal controllability is sought, particularly in the case of an Insider Threat Paradigm or ITP) as a form of mitigation. In essence, the maximal optimum Control Signal Energy Cost ($CSEC_{opt}$) and reduction of the diffusion of malicious Control Signals (CS) and/or Augmented CS (ACS) is sought. The described problem space is non-trivial, as Efficient Controllability Problems (ECP) have been shown to exhibit Non-deterministic Polynomial-time Hardness (NP-Hard), and likewise, countermeasure non-ECP are NP-Hard. This paper advances matters by leveraging a bespoke Machine Learning (ML) paradigm, comprised of a multi-Convolutional Adversarial Neural Network (CANN) Module and Particle Swarm Optimization (PSO)-based Enhanced Reinforcement Learning (RL) Component (ERLC), to better orchestrate Defensive Circuit Breakers (DCB) and leverage ML-based Protection Relay Selection (MLPRS) for more optimal Defensive Grid Re-configuration (DGR) so as to better obviate a PSHF-based ITP Sequential Topology Attack (STA). Although previously thought to be a High-Impact, Low-Frequency (HILF) event, PSHF studies have shown that the associated distribution has an unusually fat tail; by endeavoring to reduce the fat tail, a principal contribution of this paper is to lessen the impact of the involved event.**

Keywords-Cyber; supply chain vulnerability; insider threat; zero-day type vulnerabilities; hidden defects/failures; protection system hidden failure; sequential topology attack; cascading failure; blackout; resiliency; control signal energy cost; artificial intelligence; machine learning; reinforcement learning.

I. INTRODUCTION

Despite the numerous advancements in power grid protection systems, in many cases, these systems have constituted the actual problem and caused cascading failures resulting in power outages; in essence, they induced undesired effects in the very power grids they were tasked to protect. To further this irony, Protection System Hidden Failures (PSHF) are now recognized as a key amplification factor and cause of several recent major disturbances and outages. Although previously thought to be a High-Impact, Low-Frequency (HILF) event, PSHF studies now show that the associated distribution has an unusually fat tail; in essence, the frequency of manifestation has been much higher than its current classification. Some PSHF researchers construe the paradigm to actually be Very High-Impact, Medium-Frequency (VHIMF) events. To compound this issue, for contemporary times, wherein cybersecurity is a prevailing societal issue, several research studies have shown that in the counterpoising between dependability (e.g., clearing a fault on a protected element) and security (e.g., mis-operating, such as clearing a fault when a fault has not yet occurred on a protected element), the bias is skewed towards dependability/reliability. On the surface, this seems quite reasonable. However, as the Operational Technology (OT) PSHF is the equivalent of the Information Technology (IT) "0-Day," the dearth of robust progress in mitigating against PSHFs makes for a specious paradigm — PSHFs not only remain a critical security issue, but should PSHFs manifest, the involved power system reliability will experience a non-graceful degradation and likely be subject to a Bak–Tang–Wiesenfeld (BTW) cascading effect resulting in a cascading failure (i.e., outage).

Among other "perfect storm" events in the cyber threat ecosystem, particularly as pertains to the power grid, a particularly ominous one is the triumvirate of: (1) an Insider Threat Paradigm (ITP), (2) a PSHF(s) paradigm known to the involved ITP actor(s), and (3) the requisite knowledge/ability to launch a targeted (based upon knowledge of the PSHF paradigm) ITP Sequential Topology Attack (STA) to effectuate a cascading failure paradigm (e.g., outage) of the involved power grid. The described scenario would be of tremendous concern to the involved system operators, power engineers, reliability engineers, protection engineers, cyber practitioners, and resiliency engineers, among others. Each of these three paradigms, collectively comprising the undesired triumvirate amalgam, is described below.

 ISBN: 978-1-61208-996-6

A. The ITP for the Smart Grid

The ever-expanding modern "Smart" Grid (SG) creates an ever-larger attack surface area, as it incorporates a plethora of IT, the IT subset of Information and Communications Technology (ICT), the adjacent realm of OT, the OT subset of, among others, Industrial Control Systems (ICS), and the various nexuses. According to Accenture's "State of Cybersecurity Resilience 2021," cyber security-related attacks increased 31% from 2020 to 2021; more specifically, according to the Kaspersky ICS Computer Emergency Response Team (CERT), 39.6% of ICS were targeted in the second half of 2021. According to Claroty's "Biannual ICS Risk & Vulnerability Report" and its Team82, ICS vulnerabilities increased by 41%, 61% of the vulnerabilities were remotely exploitable, and 71% were classified as high/critical vulnerabilities. To aggravate matters, according to ID Watchdog, 60% of data breaches in 2020 were from ITPs. According to Techjury, 66% of organizations consider IPTs a more likely paradigm than external attacks. Also, according to Ponemon Institute's "Cost of Insider Threats: Global Report," over the last two years, the number of ITP incidents has increased by 47%. Suffice it to say, the ITP/ICS/SG amalgam within the cyber ecosystem seems to constitute a prevailing paradigm.

B. PSHF within the SG

In addition to the ITP, the SG is also beset with the equivalent of "Zero-Day" or "0-day" vulnerability exploits, which is used to describe a software, hardware, firmware, or paradigm-related vulnerability for which no mitigation yet exists; the ICS manifestation is referred to as Hidden Defects/Failures (HDF) and these include, among others, PSHFs that are not able to be detected under current Condition-Based Maintenance (CBM) instantiations. To compound the ominous nature of PSHF, according to Insights (as well as various contributors to the Carnegie Mellon University Software Engineering Institute), based upon statistics from the CERT National Insider Threat Center (NITC) Incident Corpus, "the percentage of insider incidents perpetrated by 'trusted business partners' typically ranges between 15% and 25% across all insider incident types and industry sectors." According to MITRE and DTEX Systems, there has been a 72% increase in ITP incidents between 2020 and 2021. The implication is clear; if the "trusted business partner" (that provided the protection system-related device/component, which is also known as a Security and Stability Control Device or SSCD) constitutes the ITP, then the PSHFs could, potentially, be intentional and by design. For this case, the encompassing Security and Stability Control System (SSCS) or Electric Power Alarming and Coordinated Control System (EACCS) (for which the SSCD is a constituent component) could be considered compromised. The ensuing implications could potentially be quite profound. The North American Electric Reliability Corporation (NERC) has asserted that more than 70% of major disturbances, which segue to system cascading collapses (e.g., outages), are caused by PSHF. In addition, Yankson et al. demonstrated that a 0-day can amplify the negative impact of a disturbance event by a factor of 86 with a major disturbance outcome [1]. Suffice it to say, the ITP-PSHF/ICS/SG amalgam within the cyber ecosystem seems to constitute an ominous threat.

C. STA as a Targeted ITP Attack

It was previously shown in [2], as well as by studies, such as by Guo et al. and others, that while certain Cyber Physical Systems (CPS), such as Cyber-Physical Power Systems (CPPS), can provide a modicum of resilience for high-indexed nodes, they are much less resilient to targeted attacks (e.g., ITP attacks) [3][4]. From a Supply Chain Vulnerability (SCV)/Cyber-Physical SCV(CPSCV) perspective, if a "trusted business partner" has intricate knowledge of the involved power grid (e.g., CPPS topology, EACCS, SSCS, SSCD, PSHF, etc.), then the associated CPPS (and involved EACCS and/or SSCS) resiliency against a targeted ITP attack could dramatically shift from a more desirable higher resilience number (e.g., resilience = 10 for a minimally vulnerable CPPS, EACCS, SSCS, etc.) to an undesirable lower resilience number (e.g., resilience = 0 for a maximally vulnerable CPPS) in a fashion alluded to by Silveira, et al [5]. Moreover, with such intricate knowledge, the targeted ITP attack might leverage the capability for sequential control to exploit the phenomenon in a fashion that, as Zhu et al. and others have noted, "the sequential attack is demonstrated to be statistically stronger than the simultaneous attack" [6]. Yan et al. and others seem to concur that the impact of the STA could be much more devastating than a concurrent attack and further point out that "sequential attacks require less concurrent resources to coordinate" and therefore have a lower effectuation cost (e.g., Control Signal Energy Cost or CSEC). It was previously discussed in [2] that sufficiently low CSEC for Large Complex Networked Systems (LCNS), such as CPPS or SG, may yield to an optimal controllability paradigm (in this case, advantageous for the ITP attacker to operationalize an STA); hence, the maximal optimum CSEC ($CSEC_{opt}$) is sought to block the Malicious Command and Control (C2) (collectively, MC2) of the ITP. Suffice it to say, the ITP-PSHF-STA/ICS/SG amalgam within the cyber ecosystem seems to constitute a "perfect storm."

Contending with this "perfect storm" amalgam is a non-trivial feat. After all, mitigation actions, such as leveraging defensive SSCDs (e.g., Defensive Circuit Breakers or DCBs) and facilitating Defensive Grid Re-configuration (DGR), are non-trivial to effectuate. However, a mitigation module — to maximize CSEC at certain key nodes in the form of $CSEC_{opt}$) (so as to, indeed, effectuate a non-optimal controllability paradigm for the ITP attacker), obviate (via degrade, perturb, or disrupt) the involved "perfectly planned" STA strategy, and somewhat mitigate against the involved PSHF — is explored. Accordingly, the main contribution of the paper is to introduce a multi-Convolutional Adversarial Neural Network (CANN) (i.e., CANN1 and CANN2) mitigation module designed for handling certain PSHF, whose potency can be somewhat blunted with the mitigation module's Particle Swarm Optimization (PSO)-based Enhanced Reinforcement

 ISBN: 978-1-61208-996-6

Learning (RL) Component (ERLC), which can better orchestrate DCBs and leverage ML-based Protection Relay Selection (MLPRS) for more optimal DGR so as to better obviate a PSHF-based ITP STA. The paper is structured as follows. Section I introduces the "ITP-PSHF-STA" challenge. Section II presents relevant background information and discusses the current operating environment. Section III delineates the experimental strategy behind the multi-CANN mitigation module and its subordinate PSO-based ERLC, which collectively endeavor to contend with the referenced challenge, and compares certain solvers; some preliminary experimental findings are provided. Section IV concludes with some reflections, puts forth some envisioned future work, and the acknowledgements close the paper.

II. BACKGROUND INFORMATION

Contemporary society relies upon reliable and resilient Critical Infrastructures (CI), such as the power grid [7]. The advent and prevalent usage of ICTs has led to more connected and "smarter" CPS, such as CPPS and SG. Standards are still evolving, such as exemplared by the fact that International Electrotechnical Commission (IEC) 62351 addresses some of the security issues not addressed by IEC 61850, which has been hitherto utilized to address some of the security issues of yet other standards (e.g., IEEE C37.118). Suffice it to say, the rapid convergence of IT and OT has revealed gaps in both the security and reliability paradigms. For example, The OT threat landscape presents challenges, as various cyber security professionals have noted that the current Common Vulnerability Scoring System (CVSS) is more suitable for IT than OT. According to Tenable Research, 56% of current vulnerabilities are scored as High (i.e., CVSS score of 7.0-8.9) or Critical (CVSS score of 9.0-10.0); however, more than 75% of the vulnerabilities with a score of 7 or above have "never had an exploit published against them." Meanwhile, while there are indeed robust IT domain-centric projects, such as the 0-day Tracking Project (a.k.a., Project Zero), which keeps track of 0-days with assigned Common Vulnerabilities and Exposures (CVEs) (e.g., for 2022, it lists 17 known 0-days, which have been subsequently patched, in 2021, it lists 58, in 2020, it lists 25, etc.), much more work needs to be done in the OT domain (e.g., ICS), particularly in the area of identifying, understanding, and mitigating against PSHFs (the OT equivalents of IT 0-days), which could lead to cascading failure of an involved SG. Without properly addressing PSHFs, security will remain problematic and reliability assessments can be specious; in essence, vulnerabilities in the OT domain may need to be re-prioritized — with PSHF receiving a renewed emphasis. The current operating environs is delineated in subsections A through I below.

A. The Notion of SG

Cecati et al. noted that the SG is a "concept for transforming the electric power grid by using advanced automatic control and communications techniques and other forms of information technology" [8]. Wang et al. and others have reviewed SG communications architectures [9]. Fang et al. well noted that the U.S. Energy Independence and Security Act of 2007 directed the National Institute of Standards and Technology (NIST) to coordinate the research and development of a framework to achieve interoperability, efficiency, and reliability of SG systems (e.g., EACCS, SSCS) and devices (e.g., SSCD) [10]. Kawoosa et al. and others have reviewed SG cyber security [11], and Zhao et al. and others have reviewed PSHF in the context of security and stability of the SG. However, with regards to security and stability/dependability/reliability, Barnes et al. assert that the prevailing bias is skewed towards reliability, which may be quite specious in actuality, as the associated vulnerability paradigm actually makes the involved SG quite brittle [12].

B. SG Reliability

Indeed, whether it be a SG or non-SG, reliability (i.e., "keeping the lights on") has been central for the power grid. NERC was originally formed as the North American Electric Reliability Council in 1968 (prompted by the 1965 cascading failure and ensuing blackout in the northeastern part of the U.S.) to promote reliability standards within electric utility systems. Among other NERC promoted standards is TPL-001-1 "System Performance Under Normal (No Contingency) Conditions," wherein Category A equates to "No Contingencies," Category B equates to "Events resulting in the loss of a single system element," Category C equates to "Event(s) resulting in the loss of two or more (multiple) elements," and Category D equates to "extreme event resulting in two or more (multiple) elements removed or cascading out of service." A Category B event (with continued performance after the loss of a single component) is known as an N-1 contingency. A Category C event (with continued performance after loss of two components) is further subdivided with regards to timing: (1) N-k (where k>=2) contingency for nearly simultaneous losses, and (2) N-1-1 contingency for consecutive/sequential losses.

C. Sequential Events in the SG

Perhaps, in a counter-intuitive fashion, sequential events (e.g., attacks) turn out to have greater impact than simultaneous/concurrent events. In addition, Chen et al. illuminated the fact that the loss of one element immediately raises the likelihood of losing another element under the "cluster" probability distribution [13]. Along this vein, Salim et al. also noted that adjacent/neighboring lines or exposed lines (particularly those sharing the same bus) would have a higher probability of incorrect tripping (induced by the loss of the first element) [14]. Zhu et al. utilized an IEEE 39 bus system to show that the sequential failure of two links caused an 80% power loss, while the

simultaneous failure of the links caused less than 10% power loss [6]. Yan et al. noted that, as an extension of the N-1-1 contingency, the specific targets, number of attacks, and timing of attacks (i.e., STA) could be determined by the attackers (e.g., who had knowledge of an involved PSHF paradigm) to maximize damage [15]. For this STA scenario, the involved [SCV/CPSCV] vulnerability chain (which represents the threats due to the manifestation of an existing vulnerability, such as PSHF, as well as the threats added due to the impotency of the available mitigation controls — none in the case of "0-day" or PSHF [5]) is likely to yield to the BTW cascading effect and an ensuing outage.

D. Cascading Failure of the SG Induced by PSHF

Prourbeik et al. have noted that "cascading outages are among the most severe threats to power grid stability." [16]. One of the main causes of cascading outages for the most recent series major Western Systems Coordinating Council (WSCC) events, interestingly, involved PSHF that are not able to be detected under current CBM paradigms [17]. Salim et al. have noted that most of the major cascading collapses, have been caused by PSHF [14]. Elizondo et al. have described a PSHF as "a relay that is misconfigured or fault such that it will cause the inappropriate removal of system assets during an event" [18]. Others, such as Ree, et al. have delineated PSHF as "a permanent defect that will cause a relay or a relay system to incorrectly and inappropriately remove a circuit element(s) as a direct consequence of another switching event" [19]. Yet, in a broader sense, PSHF do not simply reside within relays; the PSHF phenomenon also resides with the various protection system-related components – SSCDs, in general.

While contemporary power grids are fairly resilient against N-1 contingency single element issues, they remain highly vulnerable to N-k contingency (particularly where k>=2) multi-element issues [20]. Forensic examinations have found that several major outages were indeed caused by the PSHF of the involved Special Protection Schemes (SPS) or Remedial Action Schemes (RAS) (which are measures specifically designed to preserve the integrity of the CPPS or SG during aberrant operating conditions [21]) within the involved EACCS, SSCS, etc. The PSHF referenced are caused not only by inherent Protection Element Functionality Defects (PEFDs) within the SSCDs, but also by associated human factors (e.g., relay settings), which can lead to a degradation of the involved SPS.

E. Classifying PSHF

PSHF can be classified in a variety of ways, but they are often divided into: (1) the causes (e.g., hardware faults, software errors, logic errors, improper operation, improper maintenance, improper protection setting values, etc.), (2) the characteristics (e.g., static, dynamic, etc.), and (3) the defects — PEFDs — which are further classified as device-related faults (a.k.a., PEFD-A) and human-related faults (e.g., protection setting-related) (a.k.a., PEFD-B) [22]. PSHF have also been organized by their positioning and functional role within the EACCS or SSCS: (1) Measuring, (2) Strategy, (3) Setting, (4) Communication, and (5) Voting pattern [22]. Taking the latter issue of voting patterns, there are typically three: (1) 2 out of 3, (2) 2 out of 2, and (3) 1 out of 2. Currently, (3) is the most adopted. However, it is not able to prevent the mal-operation of the EACCS or SSCS, via the PSHF. (2) can be quite effective, as the involved SSCDs are serially connected and will only trip when both SSCDs act; this will effectively mitigate against PSHF in either of the SSCDs, but protection action failures are still possible. (1) can also be quite effective, as demonstrated by Sandoval et al. [23], but it is the least adopted due to the high cost, architectural intricacies, Operation and Maintenance (O&M) complexities, etc. Even if (1) were utilized, Albinali et al. demonstrated that it would not eliminate all PSHF mis-operations [24]. In essence, current SGs are not architected to mitigate against PSHF.

F. Ascertaining the Probability of PSHF

To ascertain the possibility of PSHF manifesting, two distinct approaches are often used to ascertain the probability of its/their existence in the involved EACCS or SSCS: (1) probability statistical method, and (2) probability model method. The probability value obtained from (1) is a fixed value, which has a notional value at a particular snapshot in time, but unfortunately, a fixed value is not able to adequately reflect the changing probability of PSHF amidst real-time operating conditions. The probability value obtained from (2) is a non-fixed/variable value, which does indeed change to reflect different operating conditions (e.g., power flow, bus voltage, system frequency). (1) is utilized more often, as it has a lower computational cost and is more timely. However, it is not as accurate as methods utilized for (2), such as the Markov model method. Yet, the Markov model method, among other methods, requires many samples to ensure accuracy, is less timely, and an assumption is made that future states do not depend on past states (which may not necessarily be true).

PSHF may also be inclusive of multiple SSCD, SSCS and/or EACCS, such as in the case of a [Protection System] Coordination Hidden Failure (PSCHF). It is difficult enough to detect PSHF by the occurrence of a single element issue, but when complicated multi-element issues occur (e.g., such as in the case of PSCHF), the involved fault judgment circuit is likely to be ineffective and cascading failures may follow.

G. Attempts to Mitigate against PSHF and/or PSCHF

To mitigate against potential PSHFs and/or PSCHFs, one approach, among others, is to identify the key lines affected by the potential PSHFs and implement mitigation measures to inhibit cascading failures and their ensuing wide-area disturbances. Artificial Intelligence (AI) has been brought to bear to help mitigate against these scenarios, with various Defect Diagnosis/Prediction Models (DDPM) proposed. AI approaches, such as those centered upon retraining, have been studied. By way of clarification, EACCS or SSCS and the involved SSCD functions — let us say, Protective Relaying (PR) — can be construed to be a Decision

Engineering (DE) problem with a clear decision – to trip or not trip. Hence, Intelligent Protective Relays (IPR), which can retrain themselves so as to not trip inappropriately, reside within the realms of AI and DE; however, this research area is still nascent, and much works remain to be done. In brief, mitigation approach vectors for PSHF and/or PSCHF are far from robust.

H. The Intensifying Protection Challenge and PSHF

The literature shows that AI and DE research has been performed in the area of islanding detection (which endeavors to ascertain when the involved microgrid is disconnected from the main grid), which is just one of the various protection issues (e.g., undesired nuisance tripping, blinding problem involving a delay or non-tripping, etc.). Various Islanding Detection Techniques (IDT) are presented in the literature and have been reviewed by Khan et al. and others; however, IDT is, likewise, still a nascent area (as are other more complex protection issues, such as PSHF and PSCHF), and failed IDT are of critical concern for system operators, power/resiliency/security engineers, etc. [25].

To aggravate matters, the increase in highly distributed Renewable Energy Sources (RES) is increasing the need for IDT, thereby necessitating more EACCS, SSCS, and their constituent SSCD; in the case of high RES, because of the varying intermittencies, fault levels will vary, and this complexity has led to an increase in nuisance tripping (as well as associated sympathetic [nuisance] trippings) when in grid mode (i.e., false positive) and a decrease of requisite tripping (e.g., blinding problem) when in islanded mode (i.e., false negative); this is known as a loss of coordination from sequentially false operations (e.g., nuisance, sympathetic, blinding, etc.) of the relays from downstream to upstream feeders [26]. This might also involve reverse power conditions [27]. In essence, cascades can be comprised of a mixture of taxonomic (i.e., upstream to downstream) as well as folksonomic (i.e., downstream to upstream) effects.

By way of contextualizing information, the International Energy Agency (IEA) asserts that by 2026, the global renewable electricity capacity is forecast to rise dramatically from 2020 levels. RES are set to account for a substantive portion of the global power capacity through 2026, and Solar PhotoVoltaics (PV) is expected to be a principal contributor. Some areas have increased their Renewable Portfolio Standards (RPS) target to 100% renewable before 2045 (e.g., California, Hawaii) [28]. The United Nations (UN) Conference of the Parties (COP) 26 Summit accelerated action towards the goals of the Paris Agreement and the UN Framework Convention on Climate Change (UNFCCC), which places an urgency on RES to operationalize the reduction of greenhouse gas emissions/concentrations (e.g., carbon dioxide) in the spirit of the Sustainable Development Goals (SDGs). The adoption of RES (a.k.a., "green energy") has made matters, regarding CPPS or SG, more complex; after all, the RES Distributed Generation (DG) aspect introduces topological paradigms, such as islanded mode. Accordingly, the varied topology (e.g., grid mode, islanded mode) will affect the magnitude and direction of the fault currents within the microgrid in differing ways, and "the low fault current during islanded mode can lead to difficulties in fault detection or long tripping times for [Over Current] OC elements" [28]. Hence, the protection challenge, and that of the involved EACCS, SSCS, and their constituent SSCD, becomes much more complicated.

To meet this challenge, an Adaptive Protection Scheme (APS) seems prudent, as APS endeavors to ascertain the state of the CPPS or SG and make adjustments to its configuration (e.g., changing relay settings), accordingly; after all, settings likely need to be different for different network operating topologies/different operating modes due to a large difference in fault currents [26][28]. Horowitz et al. and others point out the merits of APS. Others, such Gao et al. point out that even though APS might be able to reduce the potential for mis-operation (e.g., incorrect settings), such approaches will not help to protect against PSHF (and PSCHF), which are not detectable via self-tests (a.k.a., self-diagnostics) and are extremely difficult to detect even centrally/externally.

The very real underlying danger of PSHF (which should be of interest, pursuant to the spirit of Critical Infrastructure Protection (CIP)-002-4 "Cyber Security – Critical Cyber Asset," particularly as it relates to intentional/unintentional compromises of the power system [9]), is that they are hidden during normal CPPS, EACCS, SSCS, as well as SSCD operating conditions and only manifest when disturbances occur (e.g., overloads, faults, etc.). In a sense, they are comparable to the classically understood "0-day" vulnerabilities, as no mitigation is yet in place. PSHF are particularly ominous, as they can induce unnecessary outages of functional/operational SSCD, SSCS, EACCs, etc. upstream as well as downstream and are particularly pervasive; Zhang et al. provide an example of an SSCD — remote zone 3 protection relays (wherein the protection relay setting covers the first line, the longest second line, and 25% of the third line) — as being essential to power systems, but their false trips are also one of main causes related to cascading outages [29]. PSHF variations have also been increasing at an alarming rate.

By way of background, Liptak et al. nicely articulate the fact that the "the IEC 61850 logical device model allows a single physical device to act as a proxy or gateway for multiple devices[,] thus providing a standard representation of a data concentrator" [30]. The underpinning basic element, for devices and functions, is the Logical Node (LN). As the LNs are associated with a Substation Configuration Description (SCD) file, any shift in the SCD may result in Configured [Intelligent Electronic Device] IED Description (CID) changes, thereby increasing the potentialities of PSHF.

I. Devising a Detection Schema for Certain PSHF

To adequately contend with the burgeoning corpus and potentialities of PSHF, we first look at the gamut of SSCDs.

 ISBN: 978-1-61208-996-6

The NERC Standard Protection and Control (PRC)-005-6 organizes the SSCDs as follows: (1) Protective Relay (Table 1-1), (2) Communications Systems (CS) (Table 1-2), (3) Voltage and Current Sensing Devices Providing Inputs to Protective Relays (Table 1-3), (4) Protection System Station Direct Current (DC) Supply (PSSDCS) (Table 1-4), and (5) Control Circuitry Associated with Protective Functions (Table 1-5) (includes CBs — which includes DCBs —and other interrupting devices) [31].

First, for the Protective Relay (and constituent Time Delay Relays or Delay Timers), when the operating condition of the overarching SSCS changes, and the setting of the involved Relay does not change accordingly (e.g., thereby resulting in an outdated Relay setting), the Relay may not be able to accurately detect the status of the SSCS and mis-operate; with regards to the delay timers, they could fail in the "closed" position [12]. Second, for the CS, Gao et al. pointed out the heavy dependence on CS greatly reduces the reliability of the involved EACCS, SSCS, etc. [31]. Third, for the Voltage and Current Sensing Devices, we first take the Current Transformer (CT); for the CT, after a fault occurs, fault currents may cause the CT core to segue to a saturation situation, wherein the secondary current of the CT is no longer a viable proxy for the primary current. Next, we take the Voltage Transformer (VT); for the VT (e.g., Capacitor Voltage Transformer or CVT/Coupling Capacitor Voltage Transformer or CCVT), after a fault occurs, the system voltage may decrease dramatically from its prototypical baseline level to a very low-level paradigm, wherein, the secondary voltage level of the VT is no longer a viable proxy for the primary voltage level. Fourth, for the PSSDCS, were it to fail, there would likely be no power provided to the involved SSCDs in the event of an fault/outage. Fifth, for the "Control Circuitry Associated with Protective Functions, we take the Circuit Breaker (CB) (and CB's subordinate trip circuit) among others; Yang et al. explored Circuit Breaker Trip Mechanisms (CBTMs) and found that CB-related PSHF dramatically decrease the involved EACCS, SSCS, et al. reliability level; PSHF in the CBTM can cause CBs/DCBs to fail to open (i.e., trip) when required, which would obviate their usefulness [32].

The commonality of (1) through (5) is that they are all subject to, among other attack vectors, a code attack, data attack, or PSHF. It is critical that (1) and (3) provide accurate measurement data (i.e., analog data). It is also vital that (2), (4), and (5) provide an accurate status of their operational health (i.e., status data). In essence, analog data equates to measurement of system states (e.g., voltage, frequency), which are emblematic of system dynamics (which can be affected by a data attack). Status data equates to topological measurements describing the connectivity of the SG (which can be affected by a code attack). Analog and status data are both used for operational DE. A mal-operation that induces deceptive analog and/or status data can be construed as a contingency event [33]. The proper orchestration of (1) through (5) is what allows the involved EACCS, SSCS, and SSCD to operate as intended.

For this paper, the devising of a mitigation module will be limited to the Protective Relay-related Paradigm (PR2P), as various researchers, such as Cheng et al. have noted that the majority of outages have been PSHF/protective relay-related. Moustafa, et al., have noted that PSHF cause about 75% of EACCS and SSCS-related events [35]. Salim et al. concurs by noting that PSHF "have been identified as one of the main causes of system cascading collapse resulting in power system instability" [14]. Furthermore, NERC data underscore the prior assertions by illuminating the fact that the distribution of cascading failures have a "fat tail instead of an exponentially falling tail, as in a normal distribution" — meaning that it occurs far more often than thought [36].

III. EXPERIMENTATION

To contend with the ominous PR2P paradigm, Wang et al. and others have posited that RL can be advantageous when contending with these Multi-Stage DE Problems (MSDEP) (e.g., to trip or not to trip), particularly in those cases involving a high degree of uncertainty (e.g., potential ITP) [9]. However, prototypical instantiations of RL necessitate a reward function, and studies have found that it is difficult for an RL agent to avoid stagnation at local optima.

It was previously shown in [37], as well as by certain other studies, that PSO could be advantageous (given the reduced number of hyperparameters to tune while providing "good enough" near-optimum solutions in relatively few iterations for solving the involved Mixed Integer Non-Linear Programming or MINLP problems), if Adaptive Inertial Weighting (AIW) (such as effectuated via a modified GNU Octave numerical computational platform, as discussed in [38]) is utilized to prevent stagnation at local optima. This approach helps to overcome the challenge of instantiating PSO aboard a Deep Convolutional Generative Adversarial Networks (DCGAN), wherein the continuous or discontinuous hyperparameters must be converted to discrete values (e.g., integers) [39], but rounding the calculated velocities to discrete integer values lends to creating an artificial paradigm, whereby particles may stagnate prematurely at local optima [40]. As the AIW-PSO approach has a suitably high efficacy for avoiding local optima and attaining a more globally optimal solution, the utilization of modern RL techniques, such as Multi-Agent RL (MARL) and Asynchronous Actor-Critic (AAC) (wherein multiple actors are efficiently trained in parallel with varying exploration policies [e.g., Novelty Search or NS, Quality Diversity or QD, etc.] [41] and whose parameters are globally contextualized by the collective actors/agents), among others, becomes viable with relatively high efficacy. Given the PSO-based ERLC, we now refer to the involved schema as AIW-PSO-ERLC.

Efficient support for MARL, ACC, etc., with the overarching MSDEP, often necessitates contending with nonconvex optimization problems; these are, in essence, nonconvex MINLPs, which need to be transformed to convex optimization problems, via certain relaxation

 ISBN: 978-1-61208-996-6

techniques. However, the involved transformations may spawn yet other nonconvex optimization problems, thereby necessitating the use of an Enhanced Robust Convex Relaxation (ERCR) framework for the tightest possible relaxation (as previously delineated in [2] and [37], among others). Interestingly, preliminary findings indicate that a specific APS IPR schema with ERCR & AIW-PSO-ERLC atop CGAN-CANN1-CANN2 (with the Bespoke Numerical Stability Implementation or BNSI discussed in [2] and [37]) well supports MARL, AAC, etc. for $MSDEP_{opt}$ (as well as Non-Efficient Controllability Problems or NECP for $CSEC_{opt}$ and AI/ML DDPM for DCB_{opt}+$MLPRS_{opt}$+DGR_{opt}), as shown in Figure 1 below. This seems to be in tandem with the posits of Ly et al., Alhazmi, et al., and Namei et al.; they contend that leveraging DCBs, [MLPRS], and DGR can mitigate against MC2 and enhance the overall SSCS, EACCS, and CPPS/SG reliability, security, as well as resiliency [42][43][44].

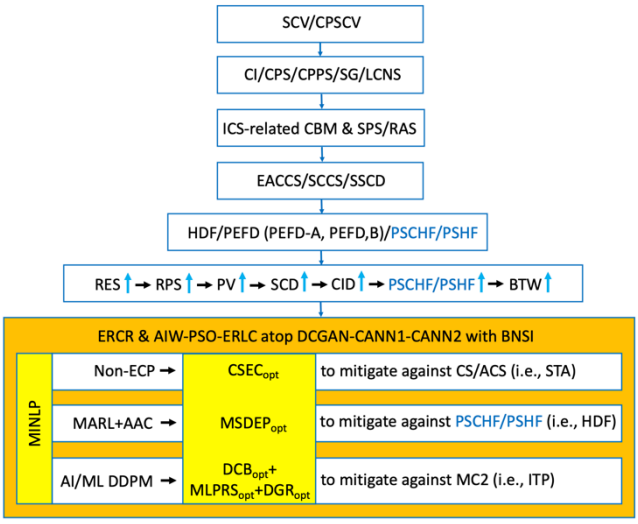

Figure 1. ERCR and AIW-PSO-ERLC atop DCGANN-CANN1-CANN2 with BNSI Framework

In essence, $CSEC_{opt}$, $MSDEP_{opt}$, and DCB_{opt}+$MLPRS_{opt}$+DGR_{opt}, among others, are — for all intents and purposes — MINLP to be resolved by the ERCR & AIW-PSO-ERLC atop DCGAN-CANN1-CANN2 with a BNSI Framework (hereinafter, referred to as the "Experimental Testbed" or ET). In resolving these particular MINLP, some mitigation of STA (for which Control Signals or CS/Augmented CS or ACS are now obviated), HDF (which includes PSHF/PSCHF), and ITP (which likely involves MC2) is effectuated. By diminishing the likelihood of PSHF/ PSCHF, the probability of a BTW cascading effect is also decreased (thereby reducing the probability of a cascading failure/outage).

In terms of some quantitative metrics, some fairly stringent experimental parameters were utilized. While certain latencies can range up to 80ms (e.g., computational processing/algorithmic execution time along with CB time) for the first zone and 500ms for the second zone [45], a maximum reporting time of 8.3ms was utilized for the involved experimentation (some Ultra-High Speed or UHS protective relays can operate at 1.5ms [46]) [47]. For practical use, the involved PR/IPR must have an Operational Time Interval (OTI) (e.g., 1.5ms < OTI < 8.3ms) that is less than the CB Interruption time, any Breaker Failure Protection (BFP) time delay (e.g., 200ms), and the Critical Clearing Time (CCT). In accordance with international standards, the PR/IPR OTI should not be much "faster than a half-cycle of power-frequency (i.e., 10ms for 50 Hz and 8.3ms for 60 Hz)" [46]; if it were, the involved CBs might not be able to operate properly [48]. Hence, a high sampling frequency (>= 1 MHz) with 1.5ms < OTI < 3ms was not desired/considered (and clearly, UHS would not be as well), as this OTI range was too fast. On the flip side, low sampling frequency PR/IPR (e.g., <1kHz to <4 kHz) with 8.3ms < OTI < 20ms was not desired/considered, as this OTI range was too slow. Medium sampling frequency PR/IPR (4 kHz to 10 kHz) with 3ms < OTI < 8.3ms had the desired OTI range.

To achieve the desired OTI range, certain nonconvex MINLP solvers and convex solvers were examined (nonconvex MINLP problems were reformulated as convex MINLP) as part of the experimentation. Comparing the nonconvex and convex solvers together, although seemingly not an equitable comparison, highlighted the potential selection bias (even as general solvers), for the described environs described herein, towards nonconvex treatment; if so, these needed to be quickly eliminated, as OTI adherence is crucial. PAVER 2.0, an open-source environment for automated performance analysis of benchmarking data, was utilized. An Experimental Solver Set (ESS) A was winnowed, and certain solvers, such as Jump Nonlinear Integer Program Solver (Juniper) were removed from further consideration due to the algorithmic execution time per problem of approximately 36 milliseconds per problem (at a batch size of 25) and about 95 milliseconds per problem (at a batch size of 100); these results were consistent with those found by Kronqvist et al [49]. The solvers of resultant ESS B, which included Basic Open-source Nonlinear Mixed Integer Programming (Bonmin), Convex Over and Under ENvelopes for Nonlinear Estimation (Couenne), mbnb, mqg, mqgpar, mglob, and Supporting Hyperplane Optimization Toolkit (SHOT), were compared; mbnb, mqg, mqgpar, are mglob are solvers available as part of the Mixed-Integer Nonlinear Optimization (Minotaur) Toolkit. The results were quite similar with regards to algorithmic execution time per problem — approximately 4 milliseconds per problem (at a batch size of 25); however, at a batch size of 100, the performance was quite different. Bonmin was eliminated, as performance ranged from 14ms+. Couenne was eliminated, as performance was at about 80ms+. Interestingly, the solvers from Minotaur all achieved performances of about sub 5ms. Likewise, the performance of SHOT was at about 4 ms. To ensure a robust resultant ESS C, the experimentation was repeated in various increments. This allowed the various solvers to both return the optimal solution and to verify optimality within the desired OTI range. In addition, the settings used by [49], as pertains to gaptol, was also utilized herein. The resultant ESS C was then further compared for performance on the ET. Of the Minotaur solvers tested, mqg

 ISBN: 978-1-61208-996-6

and mqgpar had the most consistent performance. Separately, SHOT also had consistent performance. This is shown in Figure 2 below. Hence, it seems that, for use with ET, the MILP decomposition-based solvers had better performance than Branch and Bound (BB)-based solvers; this was an interesting finding. Hence, the involved quantitative experimentation (which was partially inspired by [49]) atop ET, with the resultant ESS D, hints at the potential of certain MINLP solvers achieving near optimal solutions consistently.

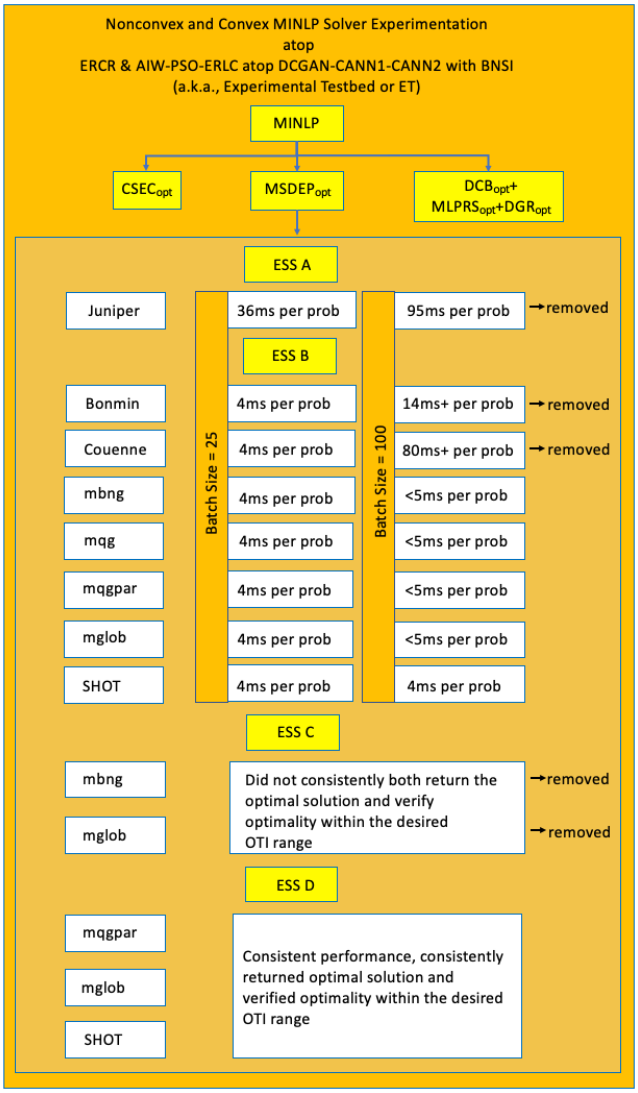

Figure 2. MINLP Experimentation atop ET

Taking the example of SHOT, it has the advantage of having robust performance for subclasses, such as Mixed Integer (MI) Nonlinear Programming (NLP) and Quadratically Constrained Quadratic Programming (QCQP). The significance of this centers upon the fact that an MINLP problem is often construed as convex when its continuous relaxation results in a convex NLP problem. Hence, SHOT's intrinsic subclass handling of the transformation from nonconvex to convex may, potentially, be more harmonious with ET, as both nicely handle those cases, wherein the involved transformations spawn yet other nonconvex optimization problems and the tightest possible relaxation is needed. Mqg and mqgpar are, likewise, quite robust.

IV. CONCLUSION AND FUTURE WORK

The OT PSHF approximates the IT "0-Day," and should PSHF manifest, it is likely to induce a BTW cascading effect, serve as a key amplification factor, and segue to cascading failure (i.e., outage). Moreover, PSHF/PSCHF-induced STA have been shown to have higher impact and cause more pervasive failures than concurrent events. This seems to be counterintuitive for many, but this lesson learned is consistent with the previously referenced findings of Zhu et al., Yan et al., and others, who have noted that the STA has greater impact than a concurrent attack (which requires a higher CSEC and more concurrent resources to coordinate). A further lesson learned is that PSHF/PSCHF-related events are not necessarily HILF events. Indeed, they seem to more closely approximate VHIMF events; this particular lesson learned seems to be affirmed by NERC, which has noted that the distribution of cascading failures occurs more frequently than envisioned. Along this vein, it seems that PSHF/PSCHF are currently underprioritized and that efforts in this area are still nascent. This seems to beget the notion that the priorities within the OT domain are quite different from those within the IT domain. A yet further lesson learned is that for certain cyber thematics, such as ITP, the prioritization seems to be higher in the IT domain than that for the OT domain.

Among other obstacles in the OT domain, leveraging ML-based workstreams and incorporating higher-level cybersecurity paradigms, amidst the predilection for seeming reliability, seems to be a challenge. An example of a higher-level paradigm is that of an apriori architected mitigation paradigm to address the ITP-PSHF-STA triumvirate amalgam. However, this seems to be absent for current SGs. This paper posits that, among others, a prospective pragmatic mitigation approach — against PR2P STA, PSHF/PSCFH, and ITP — is to intercede in the successive event stream by effectuating the maximal optimum Control Signal Energy Cost ($CSEC_{opt}$) for reducing the diffusion of CS/ACS as well as other MC2. To best mitigate against PR2P ITP, deriving DCB_{opt}+$MLPRS_{opt}$+DGR_{opt} will contribute toward reducing the efficacy of MC2 (and the associated constituent CA/ACS). This same bespoke APS IPR schema with ET and ESS D well supports deriving $MSDEP_{opt}$ to mitigate against PR2P HDF (e.g., PSHF/ PSCHF). Central to this mitigation approach is not only the AIW-PSO support for ERLC (e.g., MARL, AAC, etc.), but the encompassing bespoke multi-CANN module. Finally, the ET and ESS D also nicely address $CSEC_{opt}$ for Non-ECP so as to mitigate against CS/ACS (i.e., STA). Overall, by endeavoring to reduce the fat tail, it is the hope that the involved incidence

 ISBN: 978-1-61208-996-6

level will return to the currently anticipated/classified HILF or even better — Medium or even, ideally, Low-Impact, Low-Frequency (LILF). Future work will involve more quantitative experimentation in this area, particularly in the area of extrapolating upon the experimentation contained herein. First, further experimentation (inspired by Kronqvist et al.) involving the benchmarking of various MINLP solvers atop ET is needed. Second, further experimentation (inspired by Zhu et al., among others, which demonstrated that sequential failure of key elements causes a multiple factor greater power loss that that for simultaneous failures of the same key elements) involving the benchmarking of the STA multiple factor phenomenon is needed as well. Accordingly, mitigation approaches that satisfy the prevailing OTI constraint, such as explored herein by way of ET and ESS D, warrant further examination.

ACKNOWLEDGMENT

This research is supported by the Decision Engineering Analysis Laboratory (DEAL), an Underwatch initiative of VTIRL, VT. This is part of an ongoing VTIRL technical series, on behalf of the Quality Assurance/Quality Control (QA/QC) unit, to advance the involved TRLs.

REFERENCES

[1] S. Yankson and M. Ghamkhari, "Transactive Energy to Guard again a Zero-Day Load Altering Attack on Power Distribuion Systems," 2019 IEEE 7th International Conference on Smart Energy Grid Engineering (SEGE), 2019, pp. 171-177, doi: 10.1109/SEGE.2019.8859794.

[2] S. Chan, "Enhanced Robust Convex Relaxation Framework for Optimal Controllability of Certain Large Complex Networked Systems: An Accelerant Amalgam and Bespoke Numerical Stability Paradigm for a Decoupled and Sequenced Control Strategy on Dense and Homogeneous Temporal Networks," The 2022 IARIA Annual Congress on Frontiers in Science, Technology, Services, and Applications, ISBN: 978-1-68558-017-9.

[3] A. Guo, Y. Han, C. Guo, F. Lou, and Y. Wang, "Modeling and vulnerability analysis of cyber-physical power systems considering network topology and power flow properties," Energies, vol. 10, no. 1, p. 87, 2017, doi: 10.3390/en10010087.

[4] A. Dey, Y. Gel, and H. Poor, "What network motifs tell us about resilience and reliability of complex networks," Proc Natl Acad Sci, vol. 116, no. 39, pp. 19368-19373, doi: 10.1073/pnas.1819529116.

[5] M. Silveira, D. Dolezilek, S. Wenke, and J. Yellajousla, "Attack tree analysis of a digital secondary system in an electrical substation," 16th International Conference on Developments in Power System Protection (DPSP 2022), 2022, pp. 152-157, doi: 10.1049/icp.2022.0929.

[6] Y. Zhu, J. Yan, Y. Tang, Y. Sun, and H. He, "The Sequential Attack Against Power Grid Networks," 2014 IEEE International Conference on Communications (ICC), 2014, pp. 616-621, doi: 10.1109/ICC.2014.6883387.

[7] Y. Fang and E. Zio, "Optimizing the Resilience of Interdependent Infastructure Systems against Intentional Attacks," 2017 2nd International Conference on System Reliability and Safety (ICSRS), 2017, pp. 62-67, doi: 10.1109/ICSRS.2017.8272798.

[8] C. Cecati, G. Mokryani, A. Piccolo, and P. Siano, "An overview on the smart grid concept," IECON 2010 - 36th Annual Conference on IEEE Industrial Electronics Society, 2010, pp. 3322-3327, doi: 10.1109/IECON.2010.5675310.

[9] W. Wang, R. Wang, H. Zhang, Z. Zhou, and Y. He, "Matching Learning-Based Relay Selection for Substation Power Internet of Things," Wireless Communications and Mobile Computing, vol. 2022, Feb. 2022. https://doi.org/10.1155/2022/6795205.

[10] X. Fang, S. Misra, G. Xue, and D. Yang, "Smart Grid — The New and Improved Power Grid: A Survey," IEEE Communications Surveys & Tutorials, vol. 14, no. 4, pp. 944-980, Fourth Quarter 2012, doi: 10.1109/SURV.2011.101911.00087.

[11] A. Kawoosa and D. Prashar, "A Review of Cyber Securities in Smart Grid Technology," 2021 2nd International Conference on Computation, Automation and Knowledge Management (ICCAKM), 2021, pp. 151-156, doi: 10.1109/ICCAKM50778.2021.9357698.

[12] A. Barnes, "The Risk of Hidden Failures to the United States Electrical Grid and Potential for Mitigation," 2021 North American Power Symposium (NAPS), 2021, pp. 1-6, doi: 10.1109/NAPS52732.2021.9654709.

[13] Q. Chen and J. McCalley, "A cluster distribution as a model for estimating high-order event probabilities in power systems," 2004 International Conference on Probabilistic Methods Applied to Power Systems, 2004, pp. 622-628.

[14] N. Salim, et al., "Determination of available transfer capability with implication of cascading collapse uncertainty," IET Generation, Transmission & Distribtuion, vol 8, no. 4, pp. 705-715, Apr. 2014, doi: https://doi.org/10.1049/iet-gtd.2013.0395.

[15] J. Yan, H. He, X. Zhong, and Y. Tang, "Q-learning Based Vulnerability Analysis of Smart Grid against Sequential Topology Attacks," IEEE Transactions on Information Forensics and Security, vol. 12, no. 1, pp. 200-210, Jan. 2017, doi: 10.1109/TIFS.2016.2607701.

[16] P. Pourbeik, P. Kundur, and C. Taylor, "The anatomy of a power grid blackout – root causes and dynamics of reent major blackouts," IEEE Power and Energy Magazine, vol. 4, no. 5, pp. 22-29, Sept.-Oct. 2006, doi: 10.1109/MPAE.2006.1687814.

[17] J. Zhang, "Research on Hidden Failure Reliability Modeling of Electric Power System Protection," Energy and Power Engineering, vol. 5, 2013, doi: 10.4236/epe.2013.54B261.

[18] D. Elizondo, J. Ree, A. Phadke, and S. Horowitz, "Hidden failures in protection systems and their impact on wide-area disturbances," 2001 IEEE Power Engineering Society Winter Meeting, 2001, pp. 710-714, doi: 10.1109/PESW.2001.916941.

[19] J. Ree, Y. Liu, L. Mili, A. Phadke, and L. DaSilva, "Catastrophic Failures in Power Systems: Causes, Analyses, and Countermeasures," in Proceedings of the IEEE, vol. 93, no. 5, pp. 956-964, May 2005, doi: 10.1109/JPROC.2005.847246.

[20] K. Bae and J. Thorp, "A Stochastic Study of Hidden Failures in Power System Protection," J. Decis. Support. Syst., vol 24, no. 304, pp. 259-268, 1999, doi: https://doi.org/10.1016/S0167-9236(98)00069-4.

[21] P. Hines, H. Liao, D. Jia, and S. Talukdar, "Autonomous agents and cooperation for the control of cascading failures in electric grids," 2005 IEEE Networking, Sensing and Control, 2005., pp. 273-278, doi: 10.1109/ICNSC.2005.1461200.

[22] L. Zhao, et al., "Review and prospect of hidden failure: protection system and security and stability control system," J. Mod. Power Syst. Clean Energy, vol. 7, pp. 1735–1743, 2019. doi: 10.1007/s40565-015-0128-9.

[23] R. Sandoval, et al., "Using Fault Tree Analysis to Evaluate Protection Scheme Redundancy," 37th Annual Western

Protective Relay Conference, 2010, Accessed: Aug. 14, 2022. [Online]. Available from: https://www.semanticscholar.org/paper/Using-Fault-Tree-Analysis-to-Evaluate-Protection-Sandoval-Santana/584230d9f12239cae3e1d1b58b590138710980b7.

[24] H. Albinali et al. "A Centralized Substation Portection Scheme that Detects Hidden Failures," 2016 IEEE Power and Energy Society General Meeting (PESGM), 2016, pp. 1-5, doi: 10.1109/PESGM.2016.7741559.

[25] M. Khan, A. Haque, V. Kurukuru, and M. Saad, "Islanding detection techniques for grid-connected photovoltaic systems-A review," Renewable and Sustainable Energy Reviews, vol. 154, 2022, doi: 10.1016/j.rser.2021.111854.

[26] V. Telukunta, J. Pradham, A. Agrawal, M. Singh, and S. Srivani, "Protection Challenges Under Bulk Penetration of Renewable Energy Resources in Power Systems: A Review," CSEE Journal of Power and Energy Systems, vol. 3, no. 4, pp. 365-379, Dec. 2017, doi: 10.17775/CSEEJPES.2017.00030.

[27] V. Papspiliotopoulos, G. Korres, and N. Hatziargyriou, "An adaptive protection infrastructure for modern distribution grids with distributed generation," CIGRE Science & Engineering, February 2017, Accessed: Aug. 14, 2022. [Online]. Available from: https://e-cigre.org/share/publication/503/C6-108_2016.

[28] T. Patel and J. Hernandez-Alvidrez, "Adaptive Protection Scheme for a Real-World Microgrid with 100% Inverter-Based Resources," 2020 IEEE Kansas Power and Energy Conference (KPEC), 2020, pp. 1-6, doi: 10.1109/KPEC47870.2020.9167527.

[29] J. Zhang and Y. Dong, "Preventing False Trips of Zone 3 Protection Relays in Smart Grid," Tsinghua Scient and Technology International Journal on Information Science, vol 20, no. 2, pp. 142-154, 2015, doi: 10.1109/TST.2015.7085627.

[30] B. Liptak and H. Eren, "Instrument Engineers' Handbook: Process Software and Digital Networks," Research Triangle Park, NC, CRC Press, 2016.

[31] X. Gao, J. Thorp, and D. Hou, "Case Studies: Designing Protection Systems That Minimize Potential Hidden Failures," 2013 66th Annual Conference for Protective Relay Engineers, 2013, pp. 384-393, doi: 10.1109/CPRE.2013.6822053.

[32] F. Yang, A. P. S. Meliopoulos, G. J. Cokkinides, and Q. B. Dam, "Effects of Protection System Hidden Failures on Bulk Power System Reliability," 2006 38th North American Power Symposium, 2006, pp. 517-523, doi: 10.1109/NAPS.2006.359621.

[33] S. Tan, D. De, W. Song, J. Yang and S. Das, "Survey of Security Advances in Smart Grid: A Data Driven Approach," in IEEE Communications Surveys & Tutorials, vol. 19, no. 1, pp. 397-422, First quarter 2017, doi: 10.1109/COMST.2016.2616442.

[34] Y. Cheng, X. Chen, J. Ren, X. Xuan and X. Li, "Study on hidden failure of relay protection in power system," 2013 IEEE International Conference on Cyber Technology in Automation, Control and Intelligent Systems, 2013, pp. 434-439, doi: 10.1109/CYBER.2013.6705485.

[35] M. Moustafa and C. Chang, W. Song, J. Yang and S. Das, "Preventing cascading failure of electric power protection systems in nuclear power plant," Nuclear Engineering and Technology, vol. 53, no. 1, pp. 121-130, Jan. 2021, doi: https://doi.org/10.1016/j.net.2020.06.010.

[36] H. Liao, J. Apt, and S. Talukdar, "Phase Transitions in the Probability of Cascading Failures," Physics, 2004, Accessed: Aug. 14, 2022. [Online]. Available from: https://www.semanticscholar.org/paper/Phase-Transitions-in-the-Probability-of-Cascading-Liao-Apt/28a8ca494e5af264152c6191f6abf5b201582d39.

[37] S. Chan, M. Krunz and B. Griffin, "AI-based Robust Convex Relaxations for Supporting Diverse QoS in Next-Generation Wireless Systems," 2021 IEEE 41st International Conference on Distributed Computing Systems Workshops (ICDCSW), 2021, pp. 41-48, doi: 10.1109/ICDCSW53096.2021.00014.

[38] Chan, Steve, "Mitigation Factors for Multi-domain Resilient Networked Distributed Tessellation Communications," The Fifth International Conference on Cyber-Technologies and Cyber-Systems (CYBER 2020), 2020, p. 66-73, Accessed: Aug. 14, 2022. [Online]. Available from: https://ssrn.com/abstract=3789770.

[39] X. Liu, Q. Wang, H. Liu, and L. Li, "Particle swarm optimization with dynamic inertia weight and mutation," *2009 Third International Conference on Genetic and Evolutionary Computing*, Feb 2010, pp. 620–623, doi: 10.1109/WGEC.2009.99.

[40] C. Worasucheep, "A particle swarm optimization with stagnation detection and dispersion," *2008 IEEE Congress on Evolutionary Computation (IEEE World Congress on Computational Intelligence)*, Hong Kong, June 2008, pp. 424-429, doi: 10.1109/CEC.2008.4630832.

[41] E. Conti, V. Madhavan, F. Such, J. Lehman, K. Stanley, and J. Clune, "Improving exploration in evolution strategies for deep reinforcement learning via a population of novelty-seeking agents," Proceedings of the 32nd International Conference on Neural Information Processing Systems (NIPS), Dec. 2018, pp. 5032-5043, doi: https://dl.acm.org/doi/10.5555/3327345.3327410.

[42] K. Ly, K. Kwiat, C. Kamhoua, L. Njilla and Y. Jin, "Approximate Power Grid Protection Against False Data Injection Attacks," 2017 IEEE 15th Intl Conf on Dependable, Autonomic and Secure Computing, 15th Intl Conf on Pervasive Intelligence and Computing, 3rd Intl Conf on Big Data Intelligence and Computing and Cyber Science and Technology Congress (DASC/PiCom/DataCom/CyberSciTech), 2017, pp. 527-533, doi: 10.1109/DASC-PICom-DataCom-CyberSciTec.2017.97.

[43] M. Alhazmi, P. Dehghanian, S. Wang and B. Shinde, "Power Grid Optimal Topology Control Considering Correlations of System Uncertainties," in IEEE Transactions on Industry Applications, vol. 55, no. 6, pp. 5594-5604, Nov.-Dec. 2019, doi: 10.1109/TIA.2019.2934706.

[44] M. Nazemi, P. Dehghanian, and M. Lejeune, "A Mixed-Integer Distributionally Robust Chance-Constrained Model for Optimal Topology Control in Power Grids with Uncertain Renewables," 2019 IEEE Milan PowerTech, 2019, pp. 1-6, doi: 10.1109/PTC.2019.8810440.

[45] M. Eissa, "Resilient wide-area monitoring and protection scheme with IEEE Std. C37.118.1-2011 criteria for complex smart grid system using phase diagram," 2019 IET Smart Grid, vol 2, no. 2, pp. 309-317, 2019, doi: 10.1049/iet-stg.2018.0247.

[46] S. Zubic, Z. Gajic and D. Kralj, "Line Protection Operate Time: How Fast Shall It Be?," in IEEE Access, vol. 9, pp. 75608-75616, 2021, doi: 10.1109/ACCESS.2021.3081993.

[47] H. Wu, K. Tsakalis, and G. Heydt, "Evaluation of time delay effects to wide-area power system stabilizer design," IEEE Transactions on Power Systems, vol. 19, no. 4, pp. 1935-1941, Nov. 2004, doi: 10.1109/TPWRS.2004.836272.

[48] B. Kasztenny and J. Rostron, "Circuit breaker ratings—A primer for protection engineers," 2018 71st Annual Conference for Protective Relay Engineers (CPRE), 2018, pp. 1-13, doi: 10.1109/CPRE.2018.8349782.

[49] J. Kronqvist, D. Bernal, A. Lundell, and I. Grossman, "A review and comparison of solvers for convex MINLP," Optimization and Engineering, vol 20, pp. 397-455, 2019, doi: 10.1007/s11081-018-9411-8.

 ISBN: 978-1-61208-996-6