Data-Centric Analysis of Compound Threats to Critical Infrastructure Control Systems

Sahiti Bommareddy, Benjamin Gilby, Maher Khan, Imes Chiu, Mathaios Panteli,
John W. van de Lindt, Linton Wells II, Yair Amir, and Amy Babay

School of Computing and Information, University of Pittsburgh — {beg59, maherkhan, babay}@pitt.edu
Department of Computer Science, Johns Hopkins University — {sahiti, yairamir}@cs.jhu.edu
U.S. Army Corps of Engineers (USACE) — {imes.chiu}@usace.army.mil
Department of Electrical and Computer Engineering, University of Cyprus — {panteli.mathaios}@ucy.ac.cy
Department of Civil and Environmental Engineering, Colorado State University — {jwv}@engr.colostate.edu
Center for Resilient and Sustainable Communities (C-RASC), George Mason University — {lwells9}@gmu.edu

Abstract—**Compound threats involving cyberattacks that are targeted in the aftermath of a natural disaster pose an important emerging threat for critical infrastructure. We introduce a novel compound threat model and data-centric framework for evaluating the resilience of power grid SCADA systems to such threats. We present a case study of a compound threat involving a hurricane and follow-on cyberattack on Oahu Hawaii and analyze the ability of existing SCADA architectures to withstand this threat model. We show that no existing architecture fully addresses this threat model, and demonstrate the importance of considering compound threats in planning system deployments.**

I. Introduction

Compound threats, in which cyberattacks are targeted to compound the damage caused by natural disasters, are an increasing concern for critical infrastructure. Such threats can expand the damage caused by a natural disaster to result in wider catastrophic infrastructure failures and ecological disasters. Today, these concerns are growing more plausible: increasing infrastructure interdependencies not only make compound threats more likely, but also increase their potential impacts.

Federal, state, and local governments are paying more attention to these threats. During the 2021 Multi-State Information Sharing and Analysis Center (MS-ISAC) annual exercises, ten scenarios involved planning for the dual impact of a cyberattack and a natural disaster [1]. After Hurricane Harvey in 2017, the U.S. Army Cyber Institute conducted a three-day drill in Houston the following year simulating a cyberattack during a hurricane [1]. Cyberattacks on hospitals are also growing [2], and a recent study by George Mason University modeled the impact of such attacks on hospital operations during the COVID-19 pandemic [3]. There is an emerging trend of complex catastrophic events induced by a combination of climactic and man-made threats for the purpose of inflicting the most damage on the environment and society.

Power grid infrastructure represents a particularly important potential target for compound threats, due to the fact that many other critical infrastructures rely on power to function. Specifically considering networked control systems, such as power grid Supervisory Control and Data Acquisition (SCADA) systems, the two aspects of a compound threat (non-malicious failures due to a natural disaster, and malicious failures due to a targeted cyberattack) have different characteristics and effects on the the system. Non-malicious failures may cause parts of the infrastructure to operate in reduced capacity or to become unavailable for long periods of time (e.g. because they lost power or were physically destroyed in a climatic event). In contrast, sophisticated malicious attacks may specifically target the system components that are likely to have the greatest impact, such as central substations, power stations or even control centers. Successful intrusions (compromises) of the control servers can cause the system to behave in incorrect ways (exhibiting arbitrary/Byzantine behavior [4], [5]), as opposed to simply becoming unavailable.

Because of the differences between these two failure modes, the dependability literature has traditionally considered them separately, developing crash-fault-tolerant system architectures and protocols to address non-malicious faults (like those due to natural disasters), and Byzantine-fault-tolerant protocols to address arbitrary or malicious faults (like those due to attacks and compromises). However, the rise of compound threats, in which malicious attacks are targeted concurrently with or in the aftermath of a natural disaster, suggests a need to consider these types of faults jointly to understand system resilience to emerging compound threats and to develop system architectures capable of withstanding such threats.

In order to bridge this gap between traditional fault models, we present an initial exploration of compound threats in the context of power grid monitoring and control infrastructure. We introduce a novel compound threat model that encompasses damage due to a natural disaster and cyberattacks that include system-level intrusions and network-level attacks. We then analyze the ability of existing power-grid SCADA architectures to withstand this compound threat model. The SCADA architectures we consider include traditional architectures based on a single control center, modern fault-tolerant solutions deployed in practice, and state-of-the-art research-based solutions designed to withstand attacks and intrusions. To perform this analysis, we introduce a new data-centric analysis framework that integrates a data-based model of natural disaster effects with a concrete model of an attacker's power to determine the probability of a given system instance surviving a specific compound threat.

Using this data-centric framework, we perform a case-study analysis of an attacker attempting to disrupt a power-grid SCADA system on Oahu, Hawaii in the aftermath of a Category 2 hurricane striking the island. Our results show that while fault and intrusion-tolerant architectures deployed today or proposed in the literature offer some protection against compound threats, no existing architecture is designed to handle such threats, and none can guarantee uninterrupted operation under the full compound threat model we consider. This highlights the need to explicitly consider compound threats and design systems to cope with such threat models. By grounding our analysis in real hurricane data, we also show the importance of considering compound threats when determining the geographic placement of control centers.

The specific contributions of our work are:

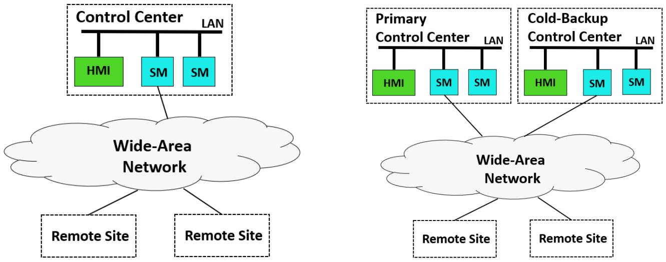
- We introduce a novel compound threat model, consisting of natural disasters and follow-on cyberattacks.
- We develop a framework for analyzing system resilience to compound threats.
- We present a case study analysis of power-grid SCADA on Oahu, Hawaii, assessing the resilience of five different SCADA configurations to compound threats involving a hurricane strike on Oahu and cyberattacks that target the SCADA system in its aftermath.
- We demonstrate the importance of considering the compound threat model in selecting system architectures and control center locations.

II. Related Work

Traditionally, frameworks for analyzing electric power grid resilience focus on risk and impact analysis of catastrophic natural disaster events [6]–[8]. Increasing concerns about malicious attacks have also led to frameworks exploring the vulnerability of the power grid to cyberattacks and their mitigation [9], [10]. While works on natural-disaster resilience generally focus on the grid's recovery to restore the power supply [11], [12], works on cyberattack analysis typically recommend measures to mitigate or prevent cyberattacks. However, these prior works have typically not focused on SCADA systems specifically. Modern grid SCADA systems are increasingly complex and interconnected to other infrastructures, thus directly impacting the power grid's resilience.

Prior work in the dependability and security literature has considered SCADA's resilience to cyberattacks and developed cyberattack-resilient SCADA systems that address Byzantine server faults and/or network attacks [13]–[17]. However, none of these works considers the compound threat model we propose. Moreover, these works do not provide frameworks for systematically evaluating their system designs in the context of real power grid deployments using data-centric fault modeling.

Some works have focused on defining and measuring the dependence between power grid SCADA and other infrastructures like communications [18]–[20]. However, to the best of our knowledge, there has not been a framework that systematically considers compound threats to grid SCADA, i.e., natural disasters and follow-on cyberattacks scenarios.



(a) Configuration "2"

(b) Configuration "2-2"

Fig. 1: Current Industry Standard Architectures

III. System and Threat Model

Our work analyzes the impact of compound threats on power grid SCADA systems. Here we introduce the SCADA system model and define the compound threat model we consider.

A. System Model

SCADA systems are responsible for the monitoring and control of power grid infrastructure. A basic SCADA architecture is shown in Figure 1a. Control servers called *SCADA Masters* (SMs), form the core of the SCADA system and are located in *control centers*. These SCADA Masters collect data from and issue commands to equipment located in *remote sites* (e.g. power plants, substations). These remote sites are geographically distributed and communicate with the SMs in the control center over a wide-area network. SMs present the state of the system to human operators through a *human machine interface* (HMI).

B. Compound Threat Model

We define a compound threat model that consists of two stages: first, a natural disaster occurs, then a cyberattack is targeted to cause further damage to the system. In the first stage of this model, the natural disaster may make one or more SCADA control centers or other control sites unavailable.[1] Although this is a generic model that can apply to any type of natural disaster, in this work, we specifically focus on hurricanes. A hurricane may render a control site unavailable by causing flooding that prevents it from operating. In addition to flooding control sites, the heavy rain and high winds produced by a hurricane may damage additional components of the power grid infrastructure (e.g. substations, transmission lines) and cause disruptions in power generation, transmission or delivery. However, we do not currently consider these in our model, as we focus on the SCADA control system.

In modeling the cyberattack part of the compound threat, we consider that the attacker can see the outcome of the natural disaster, i.e. which control sites are unavailable, and then target

[1] In the simplest architecture shown in Figure 1a, the control center is the only control site, but we also consider architectures that use multiple control centers and that use data centers as additional control sites (see Section IV-A).

their cyberattacks to cause the maximum possible damage. For the specific cyberattack model, we adopt the threat model of [16], which includes system-level intrusions and network-level attacks. Specifically, we model *server intrusion* and *site isolation* attacks. In a server intrusion, the attacker compromises a SCADA master, gaining complete control of it and causing it to behave arbitrarily (Byzantine failure).

In a site isolation attack, the attacker is able to successfully target and isolate a control site from the rest of the network, preventing it from communicating with any of the other system sites. This can be achieved through sophisticated resource-intensive denial of service attacks today [21], [22].

In our full compound threat model, we consider four specific threat scenarios, including a baseline natural-disaster-only case, and three compound threat scenarios:

- **Hurricane:** this is the baseline scenario where some control sites may be rendered non-operational due to the hurricane, but there is no cyberattack
- **Hurricane + Server Intrusion:** the attacker is able to compromise a SCADA Master after the hurricane
- **Hurricane + Site Isolation:** the attacker is able to isolate a single control site after the hurricane
- **Hurricane + Server Intrusion + Site Isolation:** the attacker is able to compromise a SCADA master and isolate a control site after the hurricane

IV. Case Study Scenario

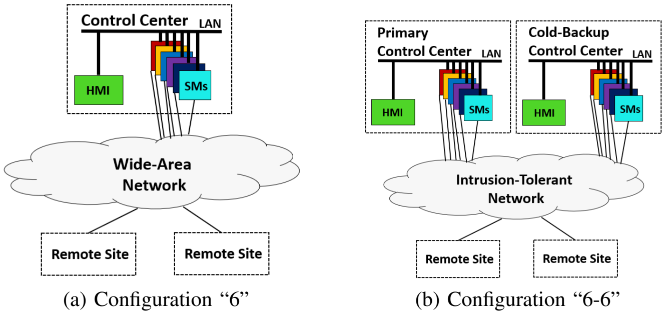
As an initial exploration of the compound threat model described in Section III, we consider a concrete case study, evaluating several existing SCADA architectures in the context of a compound threat on the power grid of Oahu, Hawaii.

A. SCADA Architectures

Prior work in [16] analyzed the resilience of a range of SCADA architectures to cyberattacks. In our analysis, we consider a subset of these architectures that offer different levels of resilience to failures and intrusions.

Industry Standard Architectures: The simplest power grid SCADA configuration we consider is a traditional single control center architecture with a primary SCADA master and a hot-backup SCADA master, as shown in Figure 1a. Following the notation in [16], we label this as configuration "2" (indicating a single site with 2 SCADA masters). This architecture is designed to withstand crashes of the primary SCADA master (by activating the hot-backup), but is not designed to withstand natural disasters or cyberattacks.

To address control center failures (e.g. due to natural disasters), many current SCADA systems use a primary-backup architecture as shown in Figure 1b. We label this as configuration "2-2" (indicating two sites, each with 2 SCADA masters). This configuration consists of a pair of SMs (primary and hot-backup) running in the primary site, and a second pair of SMs in a cold-backup site. If the primary control center fails or becomes unavailable, then the backup can be brought online, although there is a delay (on the order of minutes) to activate the cold-backup.



(a) Configuration "6" (b) Configuration "6-6"

Fig. 2: Intrusion Tolerant Architectures

Intrusion-Tolerant Architectures: The research community has introduced SCADA architectures that use intrusion-tolerant replication within a single control center to tolerate server intrusions [15], [17]. In this work, we consider the configuration "6" (Figure 2a) which uses 6 replicas to maintain safety in the presence of one server intrusion and simultaneously support one server undergoing proactive recovery [23].

To recover from a control center failure while supporting intrusion tolerance, the "6-6" configuration (Figure 2b) uses intrusion tolerant replication with 6 replicas in the primary site, and has a cold-backup control center with 6 additional replicas. Here, the primary site can tolerate a server intrusion just as "6", and if the primary site becomes unavailable (due to a natural disaster or a site isolation attack), then the cold-backup, with its own 6 replicas, can be activated (after a delay).

Network-Attack-Resilient Intrusion-Tolerant Architecture: Finally, we consider the configuration "6+6+6" (Figure 3) from [16]. This configuration is designed to simultaneously withstand both site isolation and server intrusion attacks, without incurring downtime to activate a cold backup. Six active replicas are placed in each of the two control centers and an additional six active replicas are placed in a data center to participate in the intrusion-tolerant replication protocol. The additional data center site ensures that even if one site becomes unavailable, there are enough remaining replicas to continue operations without interruption.

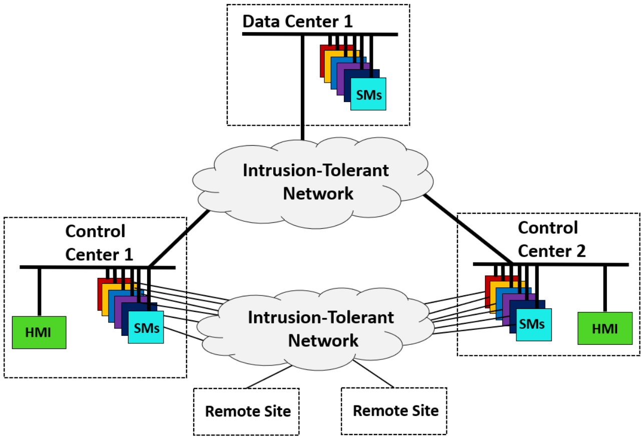


Fig. 3: Network-Attack-Resilient Intrusion-Tolerant Architecture with Configuration "6+6+6"

B. Case Study Topology: Oahu, Hawaii

For our case study, we assess the resilience of the five SCADA configurations described in Section IV-A to compound threats in Oahu, Hawaii. This is an important location for civil and military reasons. However, Oahu experiences natural disasters including hurricanes.

The power grid SCADA topology on Oahu currently includes a control center, power plants, and substations, as shown in Figure 4. For single-control-center configurations ("2" and "6"), we consider the control center to be in Honolulu. For primary-backup configurations ("2-2" and "6-6"), we locate the primary control center in Honolulu, and the backup control center in Waiau due to its geographically central location with good connectivity. For the additional data center required by the "6+6+6" configuration, we can use existing commercial data centers DRFortress or AlohaNap (labeled in Figure 4). In our analysis, we select DRFortress.

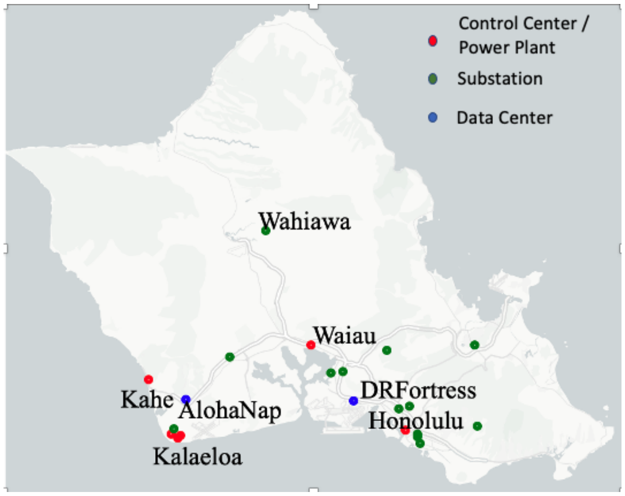


Fig. 4: Oahu, Hawaii Power Assets Topology

V. Analysis and Evaluation Framework

To analyze system resilience under our compound threat model, we built a framework whose workflow is shown in Figure 5. The analysis program takes in a SCADA topology specifying the locations of relevant SCADA assets and data detailing the impact of a natural disaster on those assets. Based on this, it derives post-natural-disaster system states. Next, a specific cyberattack model (i.e. server intrusion, site isolation, or server intrusion + site isolation) is applied to the post-natural-disaster system states to derive final system states which are evaluated and categorized into **operational states**.

We adopt the color-based state naming scheme from [16], which used similar states to capture the impact of cyberattacks on SCADA systems. For the SCADA configurations and threat model we consider, there are four possible operational states:

A **green** state indicates a fully operational system.

An **orange** state occurs in primary-backup architectures. It represents the case where the primary control center becomes unavailable, so the system will experience downtime until the cold-backup control center is activated.

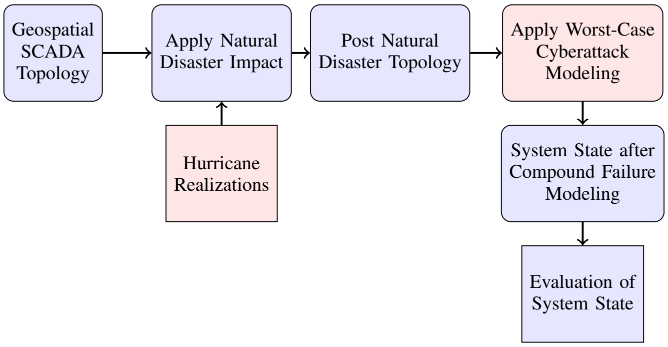

Geospatial SCADA Topology
Apply Natural Disaster Impact
Post Natural Disaster Topology
Apply Worst-Case Cyberattack Modeling
Hurricane Realizations
System State after Compound Failure Modeling
Evaluation of System State

Fig. 5: Workflow of Analysis and Evaluation Pipeline

A **red** state indicates that the system is not operational and will not be able to resume operations until some system components are repaired, or an attack ends.

Finally, a **gray** state indicates that the attacker has compromised the safety of the system, and it can behave incorrectly.

A. Hurricane Modeling

For the Oahu case study, the natural disaster input data for the framework is a set of hurricane realizations. Each realization represents a specific hurricane outcome, in which power assets may be rendered non-operational due to flooding.

To generate these hurricane realizations, we used a wave-surge model based on a simulated hurricane using the ADvanced CIRCulation Model (ADCIRC). The ADCIRC model models the inundation as a hurricane makes landfall [24]. For this analysis, we simulated a Category 2 hurricane on Oahu, using a realistic hurricane path used by emergency planners in Hawaii.

The ADCIRC model uses mesh discretization near the Oahu shoreline and then calculates the surge elevations over time as a result of a numerical model of the wind field representing the CAT 2 hurricane. Note that the mesh was coarse near the shoreline, which is quite common given the high computational demand of this modeling. This caused the results to show a water surface elevation of, for example, 1.5m, but then 0m nearby in several locations. To alleviate this discrepancy, we averaged the water surface elevations near the shoreline, and then extended the water surface elevation onto the shoreline to produce the inundation (following common practice). This provides what is typically felt to be a realistic representation of hurricane surge inundation from a storm.

The relevant power assets shown in Figure 4 were tracked to determine the inundation levels at those sites in each hurricane realization. The peak inundation from the simulated hurricane was assumed to cause the asset to fail if inundation exceeded 0.5m (2ft), since this is the typical height for switches in power plants and substations. A total of 1000 realizations were performed to generate the natural disaster input to the framework.

B. Cyberattack Modeling

As described in Section III, we consider three specific cyberattack scenarios: server intrusion, site isolation, and

	green	orange	red	gray
"2"	control center up, no intrusion	N/A	control center down/isolated	server intrusions ≥ 1
"2-2"	primary control center up, no intrusion	primary control center down/isolated, backup control center up, no intrusion	primary control center down/isolated, backup control center down/isolated	server intrusions ≥ 1
"6"	control center up, server intrusions ≤ 1	N/A	control center down/isolated	server intrusions ≥ 2
"6-6"	primary control center up, server intrusions ≤ 1	primary control center down/isolated, backup control center up, server intrusions ≤ 1	primary control center down/isolated, backup control center down/isolated	server intrusions ≥ 2
"6+6+6"	at least 2 sites up server intrusions ≤ 1	N/A	less than 2 sites up, server intrusions ≤ 1	server intrusions ≥ 2

TABLE I: Conditions determining the operational state for each SCADA configuration.

server intrusion + site isolation. We model the "worst case" cyberattacker who can see the outcome of the natural disaster and has the power to target their attack against the post-disaster system to cause the maximum damage. A simple approach to guarantee maximum damage is to analyze the results of attacking every possible combination of targets (sites and/or servers) and then choose the worst outcome as the worst case attack. However, this is computationally inefficient, so we use the following algorithm:

1) If the attacker can compromise enough servers to compromise the safety of the system, it does so.
2) Otherwise, if the attacker can isolate a site, it prioritizes isolating the primary/first control center if it is still functioning, then the backup/second control center, followed by any data centers.
3) After the attacker performs any site isolations, if the attacker has the power to perform a server intrusion, the attack compromises a server in any functioning site.

For the threat model and architectures considered, this algorithm guarantees the worst-case damage. Rule (1) guarantees that if the attacker can compromise the safety of the system, it will (leading to a gray operational state). Rule (2) guarantees that if compromising system safety is impossible, the attacker will disable the most valuable sites first (leading to a red or orange operational state if possible). Rule (3) guarantees that any intrusions are applied to servers that would otherwise have been functional, reducing the total number of operational servers as much as possible.

C. Evaluating Compound Threat Outcomes

After applying a hurricane realization and cyberattack model to a given SCADA configuration, the framework evaluates the resulting operational state. A summary of the evaluation rules can be seen in Table I.

For configuration "**2**", its operational state is *green* if the control center is functional, *red* if the control center is not functional (either due to hurricane-related flooding or a site isolation) and *gray* if there is a server intrusion.

For configuration "**2-2**", its operational state is *green* if the primary control center is functional, *orange* if the primary control center is non-functional but the backup control center is functional, *red* if both control centers are non-functional, and *gray* if there is an intrusion of a functional server.

Configuration "**6**" is identical to "2" except that it can withstand a server intrusion: an attacker is required to compromise 2 out of 6 servers to cause the gray operational state.

Configuration "**6-6**" is identical to "2-2", except, as in configuration "6", an attacker must compromise 2 servers out of the 6 servers in the currently operational site to cause the gray operational state.

For configuration "**6+6+6**", its operational state is *green* as long as at least two of its three sites are functional, and no more than one server has been compromised. If less than two sites are functional and there is no more than one intrusion in an operational server, the state is *red*. If there is more than one intrusion, the state is *gray*.

Calculating Outcome Probabilities. For each hurricane realization, the framework applies the specified cyberattack scenario and calculates the resulting operational state (i.e. green, orange, red, or gray). The probability of each operational state occurring is then calculated as the fraction of realizations that result in that state.

VI. Case Study Evaluation Results

Using the framework described in Section V, we explore each of the four threat scenarios defined in Section III. We consider SCADA control sites located in Honolulu, Waiau, and DRFortress (depending on the configuration) as described in Section IV-B. We calculate the outcome probabilities for each threat scenario as described in Section V-C.

A. Hurricane Scenario

Figure 6 shows the outcomes for all five SCADA configurations under the baseline scenario of a hurricane, with no cyberattack. In this case, the simplest configuration, using a single control center with configuration "2" has a 90.5% probability of being in a fully operational green state, and a 9.5% probability of being in a non-operational red state. This is because this architecture becomes non-operational (red) when its single control center is flooded due to the hurricane. Based on our modeling, this configuration's single control center in Honolulu is flooded due to the hurricane in 9.5% of hurricane realizations, resulting in exactly the 9.5% red probability shown in Figure 6. Surprisingly, Figure 6 shows that *none* of the other architectures is able to improve on this situation: all five configurations have 90.5% probability of

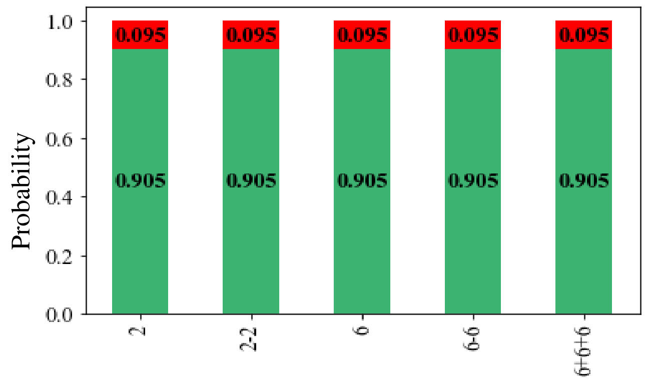


Fig. 6: Operational Profiles in Hurricane Scenario (Honolulu + Waiau + DRFortress)

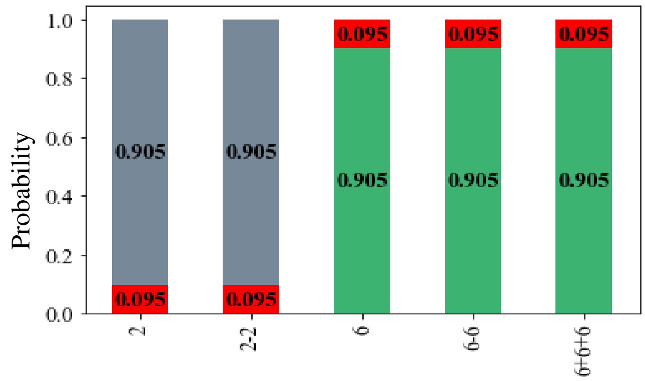


Fig. 7: Operational Profiles in Hurricane + Server Intrusion Scenario (Honolulu + Waiau + DRFortress)

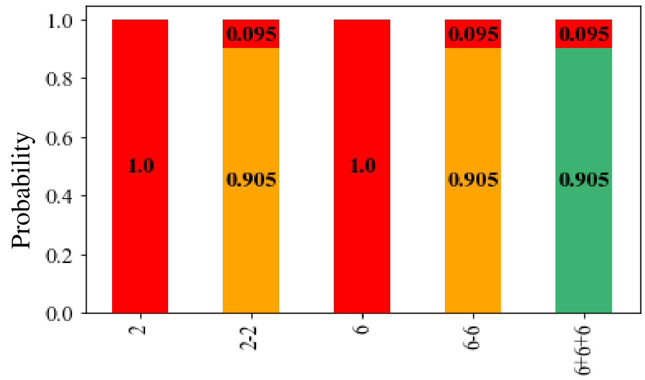


Fig. 8: Operational Profiles in Hurricane + Site Isolation Scenario (Honolulu + Waiau + DRFortress)

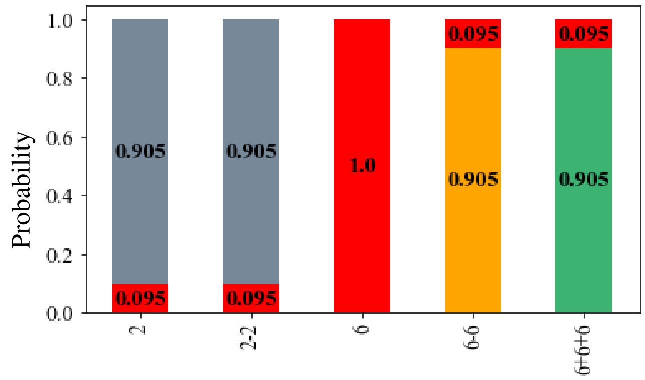


Fig. 9: Operational Profiles in Hurricane +Server instrusion + Site Isolation Scenario (Honolulu + Waiau + DRFortress)

being in a fully operational green state and 9.5% probability of being in a non-operational red state.

The main design rationale for the primary-backup system architecture (i.e. configurations “2-2” and “6-6”) is that the backup control center *should* be able to take over and restore operation if the primary control center fails. Yet, in this case we see no additional benefit from using a backup control center (or from active replication across multiple sites as in configuration “6+6+6”). This comes from the fact that, under our realistic hurricane modeling, the primary control center location in Honolulu and the backup control center location in Waiau experience strongly correlated failures. In fact, in *every* hurricane realization in which the primary control center location is flooded by the hurricane, the backup location is flooded as well. This is due to the geographic profile of the locations, which are relatively close together and at similar altitude levels. Hence, the configuration of “2-2” does not improve availability compared to configuration “2”.

The intrusion-tolerant configurations of “6”, “6-6” are designed to withstand server intrusions, but they do not provide any additional resilience to hurricane damage compared to “2” and “2-2”. While configuration “6+6+6” employs active replication across three sites to withstand the loss of any one site, this does not improve resilience in this case, since in all realizations in which the Honolulu control center is flooded, the Waiau control center is also flooded, and the configuration cannot withstand the simultaneous loss of two sites.

B. Hurricane + Server Intrusion Scenario

Figure 7 shows the outcomes for the five SCADA configurations under the compound threat scenario of a hurricane combined with a successful server intrusion. Under this threat model, the configurations “2” and “2-2” have zero probability of being in green operational state. This is expected, as these architectures are not intrusion tolerant by design. There is a 90.5% probability that the attacker is able to fully take control of the system and cause it to become incorrect (gray operational state). Interestingly, however, this probability is not 100%: if the hurricane renders the system non-operational by flooding the control center(s), there are no operational servers for the attacker to compromise and the attack cannot succeed, resulting in a red state instead of gray. This occurs in 9.5% of hurricane realizations.

In this compound threat scenario, the intrusion-tolerant configurations “6”, “6-6”, and “6+6+6” improve resilience. These configurations are designed to be fully operational in the presence of a server intrusion, and we can see that their operational profile in the presence of the hurricane + server intrusion (Figure 7) is exactly the same as with the hurricane alone (Figure 6). However, they are not explicitly designed to withstand natural disasters, and thus still have 9.5% probability of being in the non-operational red state due to the hurricane impact (as discussed in Section VI-A).

C. Hurricane + Site Isolation Scenario

Figure 8 shows the impact of a compound threat consisting of a hurricane + successful site isolation attack. The single-control-center architectures (“2” and “6”) have no ability to withstand such a threat: they are in the red non-operational state in all realizations, since even if the control center survives the hurricane, the attacker can target and isolate it.

Primary-backup architectures (“2-2” and “6-6”) can improve the situation compared to single-control-center architectures: in the realizations where both control centers survive the hurricane (90.5% of realizations), the attacker will target and isolate the primary control center, but the backup control center can be used to restore operations. However, activating the backup control center takes time, resulting in a service disruption (orange operational state) in these realizations. Compared to the hurricane alone (Figure 6), all four of these configurations have significantly worse operational profiles under the compound threat.

Of the configurations we consider, only configuration “6+6+6” does not show any degradation compared to the hurricane alone. It maintains the same operational profile of 90.5% probability of being in the green state and 9.5% probability of being in the red state. This is due to the fact that this configuration is designed to withstand any single site isolation attack with no service disruption. However, it cannot tolerate more than one site becoming unavailable, and thus is in the red operational state with 9.5% probability (realizations where both control centers are flooded).

D. Hurricane + Server Intrusion + Site Isolation Scenario

Figure 9 shows the outcomes for all five SCADA architecture with the most severe compound threat scenario, consisting of a hurricane, followed by a successful server intrusion and site isolation. Under this threat scenario, the configurations “1”, “2-2”, and “6” are always either rendered non-operational (red) or incorrect (gray). Specifically, when not rendered non-operational (red) by the hurricane, the configurations “2” and “2-2” are in gray operational state, becoming incorrect due to the server intrusion. Though configuration “6” is intrusion-tolerant, the site isolation attack renders the architecture non-operational in all realizations in which the control center was not already flooded by the hurricane, leading to 100% probability of being in a red state.

The minimum survivable configuration in this compound threat scenario is “6-6” with 90.5% probability of being in an orange operational state: it is able to withstand a server intrusion, and in the 90.5% of hurricane realizations in which both the primary and backup control center survive, the backup control center can restore operation after the primary is targeted by the site isolation attack. Configuration “6+6+6” improves on this, with 90.5% green operational state probability. This configuration is still able to maintain the same operational profile as with the hurricane alone (Figure 6). This is because it is designed to withstand the full cyberattack model of a site isolation + server intrusion. But, it is not able to withstand the full compound threat model to maintain availability (green state) in all instances; it still has 9.5% probability of being in a non-operational red state.

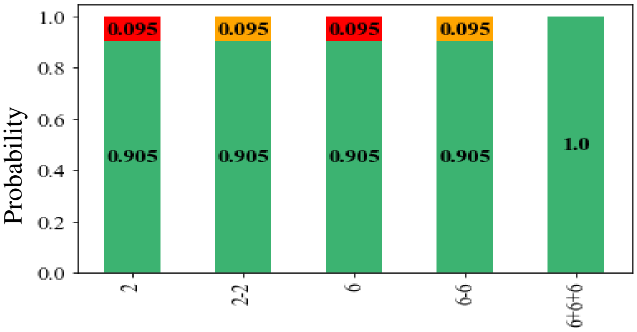


Fig. 10: Operational Profiles in Hurricane Scenario (Honolulu + Kahe + DRFortress)

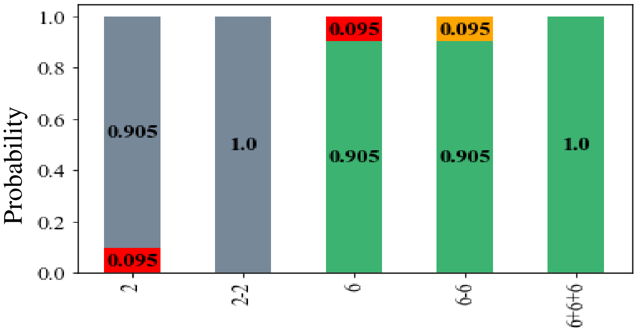


Fig. 11: Operational Profiles in Hurricane + Server Intrusion Scenario (Honolulu + Kahe + DRFortress)

VII. Discussion

Our analysis demonstrates that no existing SCADA configuration is able to fully withstand the compound threat model we consider: even the best-performing configuration “6+6+6” is not able to maintain a green fully operational state under this full threat model.

Another important outcome is that the **choice of control center locations** has a large impact on system resilience. We selected Honolulu and Waiau as the control center locations based on cyber-resilience considerations: they are locations with strong network connectivity and resources. However, their similar geographic profiles cause them to be simultaneously impacted by the hurricane under our realistic model of inundation effects.

To better understand the impact of location choices, we performed an additional analysis with Kahe as the second control center location instead of Waiau. Based on our hurricane modeling, Kahe is the site least impacted by the hurricane. As Figures 10 and 11 show, this choice can dramatically improve resilience in certain threat scenarios. Considering the hurricane alone (Figure 10), we see that configurations “2-2” and “6-6” are now able to use the backup control center at Kahe to restore operations when the primary at Honolulu fails. The 9.5% red probability for these configurations from Figure 6 is entirely converted to orange, since Kahe is never impacted by the hurricane in the realizations where the Honolulu control center is flooded. For configuration “6+6+6” the operational profile becomes entirely green.

Figure 11 shows a similar pattern for a compound threat consisting of hurricane + server intrusion, improving the profiles compared to Figure 7: configuration "6-6" can use the backup control center in Kahe to restore operation when the primary in Honolulu is flooded. Configuration "6+6+6" can maintain continuous availability (100% green state), since there are always at least two sites available when Kahe is used as the second control center. Thererfore, a question for future work is: How should we choose additional control site locations to maximize availability when increasing redundancy for compound threat scenarios?

Finally, in all threat scenarios, we assume a worst-case attacker model. While this analysis is important in understanding resilience to compound threats, it may give the attacker more power than they are likely to have in practice. How to **model realistic attacker power**, and the design implications of such an attacker model are still open questions. Future work addressing these questions can help build and deploy systems that are more resilient to compound threats.

VIII. Conclusion

We have presented a novel compound threat model, where cyberattacks are targeted to compound the damage inflicted by natural disasters. To understand the resilience of critical infrastructure to compound threats, we developed a data-centric evaluation framework. This framework determines the probability of a given system instance surviving a particular compound threat by deriving the post-natural-disaster system state from data detailing the impact of a natural disaster, and then applying the cyberattack model to the post-natural-disaster system. We used this framework to perform a case-study analysis of the resilience of power-grid SCADA systems on Oahu, Hawaii to compound threats involving an attacker attempting to disrupt the systems in the aftermath of a Category 2 hurricane striking the island. We assessed five SCADA configurations with diverse architectures, and concluded that no existing architecture can guarantee disruption-free operation under our full compound threat model. We have also shown the importance of considering compound threats and realistic disaster data when determining the geographic placement of SCADA control centers.

Acknowledgment

We thank Omar Nofal for performing the inundation analysis used as input to our framework. This work was supported by DoD Strategic Environmental Research and Development Program (SERDP) grant RC20-1138 and Installation Technology Transition Program (ITTP) project "Severe Impact Resilience".

References

[1] "Natural disasters can set the stage for cyberattacks," https://www.securityinfowatch.com/cybersecurity/news/21244746/natural-disasters-can-set-the-stage-for-cyberattacks, November 2021, retrieved March 18, 2022.

[2] "The growing threat of ransomware attacks on hospitals," https://www.aamc.org/news-insights/growing-threat-ransomware-attacks-hospitals, July 2021, retrieved March 18, 2022.

[3] H. Ghayoomi, K. Laskey, E. Miller-Hooks, C. Hooks, and M. Tariverdi, "Assessing resilience of hospitals to cyberattack," *DIGITAL HEALTH*, vol. 7, 2021. [Online]. Available: https://doi.org/10.1177/20552076211059366

[4] L. Lamport, R. Shostak, and M. Pease, "The Byzantine generals problem," *ACM Transactions on Programming Languages and Systems*, vol. 4, no. 3, pp. 382–401, 1982.

[5] M. Castro and B. Liskov, "Practical Byzantine fault tolerance and proactive recovery," *ACM Transactions on Computer Systems*, vol. 20, no. 4, pp. 398–461, Nov. 2002.

[6] S. D. Guikema, R. Nateghi, S. M. Quiring, A. Staid, A. C. Reilly, and M. Gao, "Predicting hurricane power outages to support storm response planning," *IEEE Access*, vol. 2, pp. 1364–1373, 2014.

[7] V. Krishnamurthy and A. Kwasinski, "Characterization of power system outages caused by hurricanes through localized intensity indices," in *2013 IEEE Power & Energy Society General Meeting*, 2013, pp. 1–5.

[8] M. Panteli, C. Pickering, S. Wilkinson, R. Dawson, and P. Mancarella, "Power system resilience to extreme weather: fragility modeling, probabilistic impact assessment, and adaptation measures," *IEEE Transactions on Power Systems*, vol. 32, no. 5, pp. 3747–3757, 2016.

[9] S. S. Baggott and J. R. Santos, "A risk analysis framework for cyber security and critical infrastructure protection of the us electric power grid," *Risk analysis*, vol. 40, no. 9, pp. 1744–1761, 2020.

[10] P. D. Ray, R. Harnoor, and M. Hentea, "Smart power grid security: A unified risk management approach," in *IEEE International Carnahan Conference on Security Technology*, 2010, pp. 276–285.

[11] M. Panteli, P. Mancarella, D. N. Trakas, E. Kyriakides, and N. D. Hatziargyriou, "Metrics and quantification of operational and infrastructure resilience in power systems," *IEEE Transactions on Power Systems*, vol. 32, no. 6, pp. 4732–4742, 2017.

[12] Z. Bie, Y. Lin, G. Li, and F. Li, "Battling the extreme: A study on the power system resilience," *Proceedings of the IEEE*, vol. 105, no. 7, pp. 1253–1266, 2017.

[13] V. M. Igure, S. A. Laughter, and R. D. Williams, "Security issues in scada networks," *computers & security*, vol. 25, no. 7, pp. 498–506, 2006.

[14] A. N. Bessani, P. Sousa, M. Correia, N. F. Neves, and P. Verissimo, "The CRUTIAL way of critical infrastructure protection," *IEEE Security & Privacy*, vol. 6, no. 6, pp. 44–51, 2008.

[15] J. Kirsch, S. Goose, Y. Amir, D. Wei, and P. Skare, "Survivable SCADA via intrusion-tolerant replication," *IEEE Transactions on Smart Grid*, vol. 1, no. 5, pp. 60–70, 2014.

[16] A. Babay, T. Tantillo, T. Aron, M. Platania, and Y. Amir, "Network-attack-resilient intrusion-tolerant SCADA for the power grid," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, Luxembourg City, Luxembourg, June 2018, pp. 255–266.

[17] A. Nogueira, M. Garcia, A. Bessani, and N. Neves, "On the challenges of building a BFT SCADA," in *IEEE/IFIP International Conference on Dependable Systems and Networks (DSN)*, 2018, pp. 163–170.

[18] R. Arghandeh, A. Von Meier, L. Mehrmanesh, and L. Mili, "On the definition of cyber-physical resilience in power systems," *Renewable and Sustainable Energy Reviews*, vol. 58, pp. 1060–1069, 2016.

[19] P. Chopade and M. Bikdash, "Critical infrastructure interdependency modeling: Using graph models to assess the vulnerability of smart power grid and SCADA networks," in *8th International Conference & Expo on Emerging Technologies for a Smarter World*. IEEE, 2011, pp. 1–6.

[20] J.-C. Laprie, K. Kanoun, and M. Kaâniche, "Modelling interdependencies between the electricity and information infrastructures," in *International Conference on Computer Safety, Reliability, and Security*. Springer, 2007, pp. 54–67.

[21] M. S. Kang, S. B. Lee, and V. D. Gligor, "The crossfire attack," in *2013 IEEE symposium on security and privacy*. IEEE, 2013, pp. 127–141.

[22] A. Studer and A. Perrig, "The coremelt attack," in *European Symposium on Research in Computer Security*. Springer, 2009, pp. 37–52.

[23] P. Sousa, A. N. Bessani, M. Correia, N. F. Neves, and P. Verissimo, "Highly available intrusion-tolerant services with proactive-reactive recovery," *IEEE Transactions on Parallel and Distributed Systems*, vol. 21, no. 4, pp. 452–465, 2010.

[24] R. A. Luettich, J. J. Westerink, and N. W. Scheffner, "ADCIRC: an advanced three-dimensional circulation model for shelves, coasts, and estuaries. report 1, theory and methodology of ADCIRC-2DD1 and ADCIRC-3DL," Dredging Research Program, U.S. Army Engineers Waterways Experiment Station, Vicksburg, MS, Tech. Rep. DRP-92-6, 1992.