Electric Power Grid Indications & Warning Tool

David Koester, Ph.D.
The MITRE Corporation
26 Electronic Parkway
Rome, NY 13341 USA
dkoester@mitre.org

Michael Cohen, Ph.D.
The MITRE Corporation
7525 Colshire Drive
McLean, VA 22102-7539 USA
mlc@mitre.org

Abstract*—The Electric Power grid makes an attractive target because it is the foundational critical infrastructure that underlies all others. A successful attack on the power grid causing a wide-area long-term outage would have significant national security, economic, and public health and safety consequences. Power grid outages could even cause additional cascading failures in other critical infrastructures due to the high dependency on electrical power. Hence, it is imperative that public and private authorities receive Indications and Warnings (I&W) when such attacks are in the early operational phases in order to mitigate their consequences. Towards that end, we have developed a prototype Electric Power I&W tool to provide near real-time I&W to alert private and public sector authorities when the likely causes of outage events are malicious activity. We have developed new business intelligence-style metrics to quantify the consequences of power system outages and we have developed techniques to identify multiple, cotemporaneous attacks. We demonstrate the ability to minimize false alarms due to severe weather. Similar techniques can be employed to minimize false alarms caused by high temperatures and wind or geomagnetic storms. For this capability to be used in the private and public sectors, a commercialized product based on this research would need be developed that would be: (1) part of a larger grid management capability or (2) part of state and metropolitan area fusion centers' capabilities where potential attacks on multiple critical infrastructure components are monitored continually.

I. Introduction

The Electric Power grid makes an attractive target because it is the foundational critical infrastructure that underlies all others. A successful attack on the power grid causing a wide-area long-term outage would have significant national security, economic, and public health and safety consequences [1][2]. Power grid outages could even cause additional cascading failures in other critical infrastructures due to the high dependency on electrical power [3][4]. Hence, it is imperative that public and private authorities receive Indications and Warnings (I&W) when such attacks are in the early operational phases in order to mitigate their consequences. Towards that end, we have developed a prototype tool to provide near real-time I&W to alert private and public sector authorities when the likely causes of power grid outage events are malicious activity. This prototype I&W tool compares automated messages describing grid component failures to a malicious activity profile to determine whether the likely cause is due to either natural causes/accidents or due to malicious activity. The I&W tool provides two useful outputs (1) an I&W Temporal Message stream and (2) an I&W Spatial Message stream – both triggered when metrics exceed respective thresholds.

The intent is to use this capability to detect potential attacks in near real-time in order to alert regional and national, private and public authorities in a timely manner. Having the ability to gain advance knowledge that power grid problems are due to malicious activities and not having to wait until the damage is done to determine the intentional vs. unintentional nature of the event should be a strong Homeland Security incentive to support further development of this I&W tool. The tool could be deployed as (1) a stand-alone capability, housed at a central location like the North American Electrical Reliability Corporation (NERC), with I&W messages going to DHS, DOE, and FERC, or (2) as an integrated part of every distributed electric utility's and control area's grid management capability.

In this paper, we describe the technical capabilities of our prototype I&W tool and the context where the tools have applicability. We discuss the various timeline options that are available as a function of the intended uses in section 2. Next, we describe the Resilient Grid I&W tool features. In section 4, we include discussions of how this R&D work could be productized and be used as: (1) part of a larger grid management capability incorporating all elements of an integrated Resilient Grid tool suite or (2) part of state/metropolitan area Fusion Centers' capabilities where potential attacks on multiple critical infrastructure components are monitored continually. In the concluding section, we describe our plans for further research on adapting the tool to the detection and warning of coordinated cyber-attacks on the power grid and/or Smart Grid.

II. Timeline Options for Real-Time Data Analytics

Multiple possible analytics options exist that cover the time continuum from pre-event prediction/detection to post-event forensics and historical analysis. The differences in the various analysis options are the time windows within which we are required to develop critical results. The tool we describe in this paper is best described as a post-event (post attack) near real-time indications and warnings (I&W) capability. Analytics examples along this continuum are depicted in Fig. 1. The placement of our tool in the center is not indicative of the scale

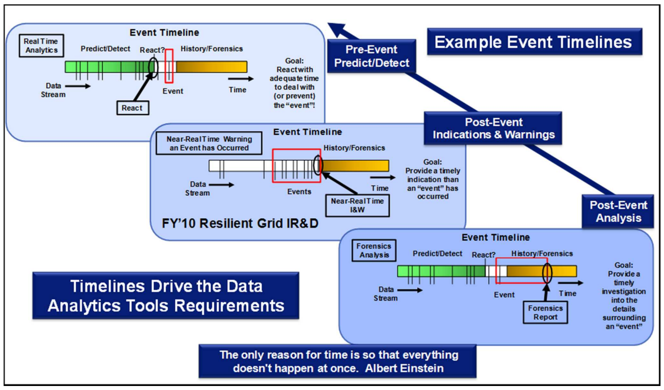

Example Event Timelines
Event Timeline
Real Time Analytics
Predict/Detect
React?
History/Forensics
Data Stream
React
Event
Time
Goal: React with adequate time to deal with (or prevent) the "event"!
Pre-Event Predict/Detect
Event Timeline
Near-RealTime Warning an Event has Occurred
History/Forensics
Data Stream
Events
Time
Near-RealTime I&W
Goal: Provide a timely indication than an "event" has occurred
Post-Event Indications & Warnings
FY'10 Resilient Grid IR&D
Post-Event Analysis
Event Timeline
Forensics Analysis
Predict/Detect
React?
History/Forensics
Data Stream
Event
Time
Forensics Report
Goal: Provide a timely investigation into the details surrounding an "event"
Timelines Drive the Data Analytics Tools Requirements
The only reason for time is so that everything doesn't happen at once. Albert Einstein

Fig. 1. Example Event Timelines

on the overall continuum. To obtain near real-time performance, we use complex event stream processing to implement metrics that identify cotemporaneous failures or failures that fall within a time window – activities that match a suspected coordinated terrorist attack profile – to identify the possibility of malicious activity. Other attack profiles would require different metrics and possible significantly more complex pattern matching and analysis.

III. Resilient Grid I&W Tool

The features of our I&W tool include:

- Metrics
    - Multiple, cotemporaneous attack profile
        - Consequence (transmission line, substation, and generator failures)
        - Ephemeral
        - False positive mitigation
    - Confidence levels based on simple frequency of arrival
    - Spatial attack profile detection
- Scenarios
    - Baseline with multiple, cotemporaneous malicious events
    - Baseline with external considerations
    - Combined
- Inputs
    - Simplified grid component failure messages
    - External considerations (severe weather/thunderstorms)
- Display dashboard
- Outputs
    - I&W message for multiple, cotemporaneous attack profile
    - I&W messages for spatial attack profile
    - Simple confidence/plausibility coefficients

Selected features listed above will be described in greater detail below.

A. Metrics to Identify Multiple, Cotemporaneous Attacks

Our I&W tool is based on a business intelligence-like metric [5] to identify suspected attack profiles. This metric must quantify the consequence of failures in the power grid as a function of their value in the system – we assume that larger capacity components have a great consequence if they fail. Meanwhile, it will be important to include external information on natural events that may significantly increase the probabilities of failures in the grid – especially in a localized area. It will be important that we quantify the confidence that our generated warning message actually represents a malicious attack. We do this by calculating a numerical confidence coefficient and relate the numerical value to a qualitative descriptor of confidence. Lastly, there is an interest in identifying two specific attack profiles – (1) a spatially focused attack and (2) a spatially diverse attack. Each of these will be described in some detail below.

A1. A Time-lagging (Ephemeral) Weighted Average (Composite) Metric

As the basis for our first simple decision process, we define a composite ephemeral metric designed to capture grid status based on:

1. "Consequence" as a weighting factor that allows the comparison of various components in the electrical grid:
    - Generators
    - Substations
    - Transmission lines
2. "Ephemeral limiting/weighting factors"
    - Time – we assume here that the profile of malicious attacks will be cotemporaneous to maximize impact on the grid and to cause cascading outages that maximize the impact of the attacks. Our metric identifies failures that occur in a short time window anywhere within an interconnection. Other metric implementations are possible– e.g., failures that attempt to maximize effect as a result of diurnal usage of electricity in varying time zones.
3. "External fused data" as a weighting factor of consequence to minimize the possibility of false alarms when identifying potential malicious activity
    - Transient events – e.g., severe weather, thunderstorms
    - Environmental events – e.g., high temperatures, cloud cover, high/calm winds
    - Large-scale but rare events – e.g., high magnetic K associated with geomagnetic storms, earthquakes, hurricanes, tropical storms

This composite metric is analogous to high-level business intelligence metrics, where the decisions to implement actions are triggered when the value of the metric exceeds a threshold [6]. Our threshold has been chosen to trigger if and when two very large grid components or when an additional number of smaller grid components fail nearly simultaneously [7].

Consider a time lagging, ephemeral metric of the form

$$\rho_{t_c} = \sum_{t_i=(t_c-\delta)}^{t_c} \gamma_{t_i} \sum_{j=1}^{n_{t_i}} \omega_{t_{i,j}} \qquad (1)$$

Where:

- ρ_{t_c} is the composite metric for time t_c
- t_c is the current time – also the end of the interval being examined
- δ is the size of the ephemeral time window
- $(t_c - \delta)$ is the first interval in the ephemeral time window
- $n_{t_i}$is the number of simultaneous events at time t_i
- γ_{t_i} is the ephemeral time weighting coefficient for time t_i
- $\omega_{t_{i,j}}$ is the consequence (for the loss of the j^{th} resource) weighting coefficient for time t_i

To account for the fact that time is continuous and we are breaking time into discrete windows, we must be careful to include a mechanism that can account for multiple failure messages within a time window in the metric. This accounts for the inner summation and the added index in $\omega_{t_{i,j}}$. For those time intervals that have no events, the consequence coefficient would be equal to zero, resulting in no contribution to the composite metric. We are assuming in this metric that the importance of individual events decays over time. The ephemeral weighting coefficient γ_{t_i}will reduce the significance of specific events to the metric as time progresses. For this implementation, the ephemeral weighting coefficient is considered independent of the events in the time interval.

In our implementation, consequence is calculated as follows:

- Generator $\omega_{t_{i,j}}$= ((MaxCap / 3000) x 10) (2)
- Substation $\omega_{t_{i,j}}$= ((Σ TxLine / (n x 1000)) x 10) (3)
- Tx Line $\omega_{t_{i,j}}$= ((TxLine / 1000) x 10) (4)

Where:

- $\omega_{t_{i,j}}$ is the consequence (for the loss of the j^{th} resource) weighting coefficient for time t_i
- MaxCap is the maximum generation capability of the failed generator unit
- Σ TxLine is the sum of the voltages of all the transmission lines attached to a failed substation
- TxLine is the voltage level of the failed transmission line

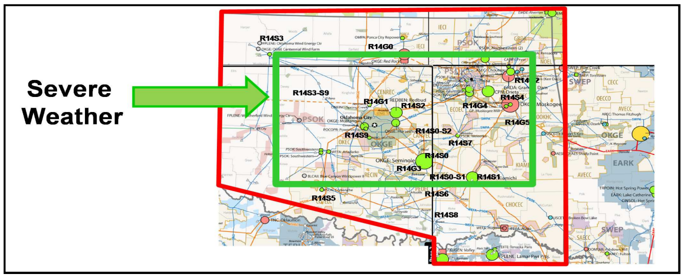


Fig. 2. Representation of a Severe Weather Warning

Our intent is to normalize the consequence of a loss of the three component types to a similar scale, where $\omega_{t_{i,j}}$ has a maximum value of approximately 10.0. Although the loss of these three component types is independent of the type of malicious cause in the formulas above, due to the large size of these components the likelihood is higher that the cause is a physical rather than a Cyber-attack.

A2 Data Fusion

A crucial portion of this spiral development was to include the ability to fuse external information to minimize false alarms. We will employ discrete logic to identify specific/certain phenomenon that indicate that activity is a result of causes other than our suspected attack profile. We implemented this as follows for severe weather – although the technique is compatible with other factors such as the impacts of the combination of temperature and wind and the impacts of phenomenon like geomagnetic storms. We represent an area with severe weather as a rectangle as can be seen in fig. 2. We check all power grid component failures to determine whether or not the component is within the box and then we attenuate the consequence value as follows:

- If inside the rectangle then ($\omega_{t_{i,j}}$ = $\omega_{t_{i,j}}$ x 0.25) (5)

In this work we have used only a single, constant attenuation value for the various grid components. If required, we could define the attenuating coefficient to be a function of one or more variables.

B. *Confidence Coefficients*

We developed probability-like confidence coefficients to accompany I&W warnings issued when our ephemeral metric determined that there is a likelihood that conditions for our multiple, cotemporaneous attack profile have been met. We examine grid status based on the frequency of occurrence of both natural and malicious events and compare the sequence of events used in calculating the composite metric to historical failure data to determine the likelihood that multiple failures are within statistical norms. The confidence coefficients are another ephemeral metric – significantly less complicated than the first metric. In theory, having two different metric values – calculated with separate logic – will minimize false positives and improve the user confidence of the I&W messages. The rules1 in our implementation:

- Allow one failure in a transmission line of 138kV and greater, or one failure in a substation with two or more lines 138kV and greater in a time window
- Generators have no failure tolerance
- Confidence coefficients are the sum of one minus the "pseudo-probabilities" that subsequent multiple failures are caused by natural events

The pseudo-probabilities that failures are caused by natural events are based on historical data. We use the calculated confidence coefficient values to generate qualitative confidence descriptions to be sent with our I&W message alerting of the multiple, cotemporaneous attack profile. The qualitative confidence coefficient values range from "Low" to "Very High

C. Spatial Attack Profiles

We developed the capability to identify specific attack profiles – based on the spatial distribution of suspected malicious events. To determine the spatial distribution of suspected malicious events, we examine failures as a function of Reliability Coordinator area and employ logic to identify whether the pattern of failures indicates that activity is a result of one of two malicious attack profiles:

- Excessive amounts of failures within a single Reliability Coordination region could indicate an attempt to overwhelm the one-off contingency operational plan and cause a cascading outage emanating out of single region
- Uniformly distributed failures in a large number of Reliability Coordination regions could indicate a geographically diverse attempt to attack the grid at an Interconnection-wide level and cause a wide area cascading outage

The implementation to determine whether or not we have encountered either of these attack profiles is straight forward. We employ a moving window to form a histogram to track the aggregate number of failures in each Reliability Coordinator area. Simple logic is employed to determine whether there is an indication of either spatial attack profile. The threshold for a spatially-focused attack is when a predetermined number or greater of failures (e.g., seven or more) occur within a time window. The threshold for a spatially-diverse attack is when a predetermined number or greater (e.g., seven or more) Reliability Coordinator areas have one or more failures within the time window. To minimize false alarms, we eliminate any failure from the histogram that is identified to fall within the external consideration area. We issue separate I&W spatial attack messages for each profile.

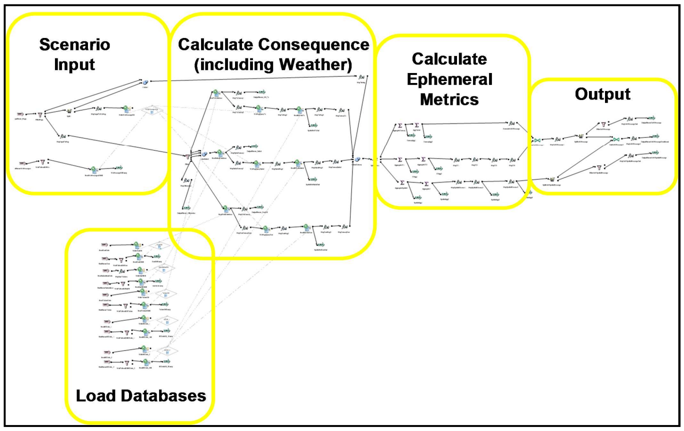

Scenario Input
Calculate Consequence (including Weather)
Calculate Ephemeral Metrics
Output
Load Databases

Fig. 3. StreamBase I&W Implementation

D. The I&W Application

The I&W Spiral Development v1.0 has been implemented in StreamBase version 6.6. StreamBase is a complex event stream processing engine where applications are developed using a graphical programming environment. After developing the resource data and input formats, it was easy to develop the application. The most recent spiral development has five major components:

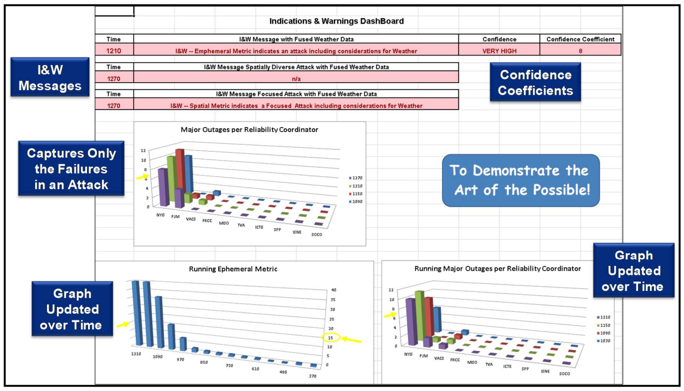
- Load Databases
- Scenario Input
- Calculate Consequence (including weather information)
- Calculate Ephemeral Metrics
- Output

The Output section provided three output streams:

- An I&W Message Stream – sent only when the multiple, cotemporaneous attack profile ephemeral metric triggers a message
- An I&W Spatial Message Stream– sent only when the spatial attack profile ephemeral metric triggers a message
- A Research Data Stream – extensive data for detailed analysis of the tool sent at a specified rate

The implementation is represented in fig. 3 where these five major components are highlighted. Icons represent actions and arrows represent data flows through the application. The programming paradigm with a complex event stream processing engine is to manipulate the content of information "*tuples*" as they flow through the application. To develop our I&W application, all we were required to do was identify the actions required and enter logic and "business" rules into dialog boxes as simple text in the StreamBase development environment. The iconic programming style greatly simplified the implementation and enabled rapid prototyping to test concepts.

[1] These rules have been developed solely for our I&W tool and do not represent logic currently used to manage the power grid.



Indications & Warnings DashBoard

Time	I&W Message with Fused Weather Data	Confidence	Confidence Coefficient
1210	I&W -- Emphemeral Metric indicates an attack including considerations for Weather	VERY HIGH	8

Time	I&W Message Spatially Diverse Attack with Fused Weather Data
1270	n/a

Time	I&W Message Focused Attack with Fused Weather Data
1270	I&W -- Spatial Metric indicates a Focused Attack including considerations for Weather

I&W Messages

Confidence Coefficients

Captures Only the Failures in an Attack

To Demonstrate the Art of the Possible!

Graph Updated over Time

Graph Updated over Time

Fig. 4. High-Level Indications and Warnings Dashboard

There is much detail in the StreamBase I&W application that simply is not possible to readily present in this format. Please contact the authors for a detailed description of the StreamBase implementation.

Lessons learned from the StreamBase Spiral Development v1.0 included (but are not limited to):

- StreamBase capabilities simplified application development
- Complex event, stream processing is a distinctive programming model – an interesting dataflow programming application [8]
- Due to the fact that we easily ran at 10x real-time speeds on a laptop for demonstrations – processing for an entire Interconnection should be able to scale out and still run effectively on a single server
- Fused external considerations
    - It was easy to implement fused external considerations even for complicated metrics
    - The method used to account for the potential effects of severe weather are extensible to other external considerations
- If productized, after we detect the multiple, cotemporaneous attacks, we would need to modify the application context to a "post" deliberate malicious attack mode -- that would look for cascading outages to correctly identify equipment failure causation.

E. Dashboard

Our Dashboard was partitioned into a High-Level Indications and Warnings Dashboard and a Research Dashboard. Fig. 4 shows the High-Level Indications and Warnings Dashboard. We have added detailed comments on the Dashboard figure. The image depicted in this Dashboard screen shot is from a point adequately into the scenario to illustrate the phenomenon of interest.

IV. Productization

A successful attack on the power grid would have significant national security, economic, and public health and safety consequences. We developed this prototype I&W tool to demonstrate the potential of such a system to rapidly identify likely malicious attacks and provide information with little delay to maximize the ability to mitigate the ongoing consequences of the initial impact. For this capability to be used in the private and public sectors, a commercialized product based on this R&D would need to be developed that would be: (1) part of a larger grid management capability incorporating additional elements of an integrated Resilient Grid tool suite or (2) part of state and metropolitan area fusion centers' capabilities where potential attacks on multiple critical infrastructure components are monitored continually.

A. An Integrated Resilient Grid Tool Suite

When deployed as an integrated tool suite, the process flow would be as follows:

1. Grid State Estimation to obtain accurate information on the grid state
2. Multiple Contingency Analysis to look beyond the current practice of "one-off" contingencies in order to prevent or minimize long lasting damage to the electric power critical infrastructure
3. Near Real-Time Look-Ahead capability to identify solutions to mitigate large-scale cascades and provide detailed causation information on failures
4. Near Real-Time I&W to alert private and public sector authorities when the likely cause of an outage is a malicious/terrorist attack

Although it could stand alone, our I&W tool would be enriched by having the advantage of information from the integrated suite of proposed applications. Further analysis of the post attack phase could identify likely failures due to cascading outages or additional malicious activity. Our I&W tool could be integrated into new grid management capabilities like new statistical grid management that will be required as renewable energy sources and "Smart Grid" features become widespread. Statistical grid management will require real-time input data on various weather sources similar to those described in this paper to determine possible wind or solar generation production or increased/decreased load. In such an instance, our I&W tool could run using the same weather data streams as those used for grid management.

B. Integration into Fusion Centers' Capabilities

For those state and metropolitan area data fusion centers tasked with monitoring activities in the region with the intent of detecting anomalous behavior that would signal hazardous situations, our tool could be critical in detecting malicious activity that is a precursor to or a part of a larger attack. We anticipate that large-scale, organized malicious activity will involve attacks on the electric power grid because it is the foundational critical infrastructure that underlies all other infrastructures. Having a tool that will detect potential malicious activity and provide indications and warnings of the situation could provide timely information to activate local emergency response plans. Capabilities that support data fusion to minimize false alarms could be enhanced to provide state or metropolitan area governments with the additional capabilities to geographically visualize the effects of severe weather or geomagnetic interference on the power grid in addition to providing indications and warnings of malicious activity.

V. Future Research

In the future, we hope to further enhance our I&W tool after community feedback. We plan to develop a concept of operations that describes how our I&W tool could be integrated with other grid management software located at reliability coordinator facilities. We also plan to describe how our external data fusion work could be used in a statistical grid management tool.

We are also examining the development a new class of real-time, domain knowledge-enhanced Cyber-attack Warning and Protection (W&P) tools that combine cyber-attack profiling with power grid domain and operational knowledge to identify one or more simultaneous critical cyber-attacks in progress before such attacks can cause physical infrastructure damage or disastrous cascading power grid outages. Like the I&W tool, we will develop the real-time, event-driven analytics tools using complex event processing technology employing context accumulation and data-fusion concepts. We will examine a series of tools that will be deployed at various locations throughout the hierarchical power grid management structure. We will examine whether separate tools will be required for (1) Balancing Authorities (131 nationwide), (2) Reliability Coordinators (17 nationwide), and (3) NERC HQ. Each version of the W&P tool will have different "views" of the power grid available and thus have different computational requirements. Having the ability to provide advance warning of a Cyber-attack at the local, regional, and national levels will be major advance over the capabilities that private and public authorities have in place today.

References

[1] D. H. Meyer, et.al. "Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations", April 2004.

[2] T. Grondin, et.al. "Power Blackout Risks: Risk Management Options", CRO Forum, November 2012.

[3] R. Zimmerman and C. E. Restrepo, "Analyzing Cascading Effects within Infrastructure Sectors for Consequence Reduction." Proceedings of the HST 2009 IEEE Conference on Technologies for Homeland Security, Waltham, MA, pp. 165-170. doi: 10.1109/THS.2009.5168029.

[4] G. H. Kjølle, I. B. Utne, and O. Gjerde, "Risk analysis of critical infrastructures emphasizing electricity supply and interdependencies", Reliability Engineering and System Safety (2012), doi:10.1016/j.ress.2012.02.006.

[5] M. Gualtieri and J. R. Rymer, "The Forrester Wave™: Complex Event Processing (CEP) Platforms", August 2009.

[6] B. Giffords and M. Palmer, "StreamBase White Paper: Real-time Profit and Loss", 2008.

[7] D. Koester and M. Cohen, "The Resilient Grid FY'10 Final Report: Resilient Electric Power Grid Operations under All-Hazard Conditions", 2010.

[8] N. Jain, et.al. "Towards a Streaming SQL Standard", 2008.