Proceedings of the 52nd Hawaii International Conference on System Sciences | 2019

Microgrid Disaster Resiliency Analysis: Reducing Costs in Continuity of Operations (COOP) Planning

Robert K. Abercrombie
Prime Time Computing, LLC
abercrombier@ieee.org

T. Benjamin Ollis
Oak Ridge National Laboratory
ollistb@ornl.gov

Frederick T. Sheldon
Ananth A. Jillepalli
University of Idaho
sheldon@ieee.org
ajillepali@uidaho.edu

Abstract

The electric grid serves a vital role in the supply chain of nearly all industrial and commercial organizations. A Microgrid infrastructure can provide this service and beneficial non-emergency services including a variety of generation/energy sources. To demonstrate the applicability of microgrids for energy resiliency, we present a microgrid resiliency case study for United Parcel Service's (UPS) three separate shipping facilities. The goal, to enhance energy security, minimize cost and prevent cascading losses within other related business units. The impacts and consequences of which are quantified in this study using a Mean Failure Cost (MFC) risk assessment measure. MFC accounts for the potential loses to identified stakeholders that may result from a set of identified failures due to a set of identified threats. In this case, our study uses a method we call All Hazards Econometric System (AHES). AHES incorporates the cost of COOP using a strategy that considers the payback period of microgrid installation as compared to other energy delivery strategies.

1. Introduction

Industrial-scale microgrids offer increased resilience, reduced risk, and enhanced controls for critical plant loads and operations, as well as the local electric grid. This paper will demonstrate methods for calculating risk, designing a microgrid, and normal operation cost recovery.

Electrical outages affect millions of customers in the U.S. every year. Increasing the resilience to natural and man-made events of the electric grid can have far-reaching societal benefits. Some of the largest individual consumers of electricity are industrial facilities. Industrial customers require highly reliable power to properly do business, and an electrical outage at the wrong moment can cause losses in the millions of dollars per hour.

Many facilities have backup generation, which is both simple and proven. However, as the electric grid modernizes, the use of microgrids as a backup system can provide benefits to both the facility and the electric grid. Benefits to an industrial customer with an installed microgrid include: 1) reduced risk from natural and man-made grid outages; 2) enhanced resilience to abnormal grid conditions; and 3) integration and optimization of energy generation sources for more efficient and economical operation.

1.1. Reduction in Risk

Every facility has risk from loss of energy supply. These risks are numerous, and it is up to the business manager to make "informed choices" on where and when to spend finite resources to protect the entire facility with regards to mitigating the risk of outages and thus addressing energy assurance.

Microgrid designs are also numerous, and can range from small, cheap installations that mitigate some risk to very large, expensive installations which significantly reduce facility risk. Using a value-based metric, this paper quantifies the risk of an enterprise system for each stakeholder based on the amount of loss that results from security threats and vulnerabilities.

This study was sponsored by U.S. Department of Energy (DOE) Grid Modernization Initiative (GMI) as a U.S. DOE Grid Modernization Laboratory Consortium (GMLC) Award.

URI: https://hdl.handle.net/10125/59789
ISBN: 978-0-9981331-2-6

1.2. Enhanced Resiliency

In the event of energy supply loss, a sufficiently sized microgrid can continue to operate the facility, independent of the state of the electric grid supply chain. Large facilities require advanced controls and coordination of assets to operate in an islanded mode, but the facility gains resiliency and reduces downtime.

Many facilities have some form of backup generation for critical loads, like emergency lighting. Microgrids can be designed to run the entire facility without grid power for days, hours, or just long enough to gracefully shut down the equipment to avoid damage and loss of inventory. This paper investigates microgrid designs which cover both ends of the continuum and quantify their impacts.

1.3. Integration and Optimization

A microgrid installation typically involves the collection and communication of multiple measurements and device parameters to a controller, which coordinates the generation and loads. A microgrid can allow for more active control over a facility, by interacting with the process control system to reduce inactive processes based on available generation for peak load reduction. Microgrid installations can now achieve this goal while addressing operational goals that include reliability improvements, cost reduction and market participation [1].

Microgrids also enable integration of many different types of fuel sources, diversifying the generation mix while reducing the probability of single points of failure. Solar arrays, natural gas turbines, diesel engines, and battery storage each have properties which can be beneficial to the reliability and resilience of a facility. A mix of generation resources can help to mask the resources' individual deficiencies, such as intermittency, long startup times, and inefficient operation. For example, a software optimizer can capture device behaviors to allow for automatic control of resources toward a common goal.

1.4. Utility Participation

Utilities base the rate they charge industrial customers via specific utility program parameters (e.g., cost/kWh during peak load periods). By participating in utility programs, industrial customers seek a positive return on their investment (ROI) during grid operations while simultaneously contributing a needed service to the grid. Instead of a rarely used backup, the generation can have a more active role in maintaining the stability and resilience of the local power system.

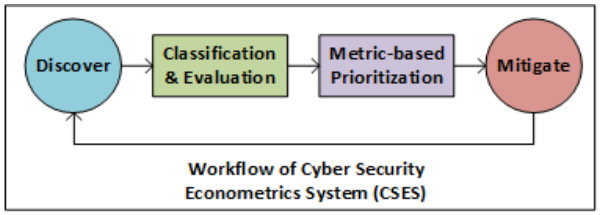

Figure 1: The Workflow of Cyber Security Econometrics System (CSES)

During grid operations, an industrial microgrid allows for more active industrial customer participation in utility programs. During peak demands, utilities make requests of their industry partners such as demand reduction. A request for demand reduction can be achieved through either the industry partner shedding load or increasing generation. The microgrid gives flexibility to the industrial customer in how to best achieve the desired load reduction.

1.5. United Parcel Service (UPS) Study

As a partner in the study [2], the UPS Worldport, Centennial Hub, and Supply Chain Solutions (SCS) campus in Louisville, KY demonstrated the validity of the approach described here.

The facility's risk mitigation strategy was determined using the All Hazards Econometrics System (AHES) method. AHES was used to evaluate the ROI for two microgrid improvement options. The first was a reduced operational sort (i.e., closing down certain sorting lanes) and the second solution considered additional resources to allow continued normal operations. AHES is an adaption of the Cyber Security Econometrics System (CSES) [3]. CSES's high-level workflow is illustrated in Figure 1. For each of these (fairly) different facilities, multiple microgrid improvement options were modeled with the open-source Sandia National Laboratories (SNL) Microgrid Design Toolkit [4]. Each microgrid solution ranged from a lower cost, with a small reliability improvement, to a more expensive cost, with a high reliability improvement. Combining these two methods and tools resulted in a newly developed approach for predicting and mitigating industrial "peak" loads. We estimated resiliency improvement, installed cost and cost avoidance for each proposed risk mitigation strategy along with a coincidental cost recovery benefit derived from normal microgrid operations.

2. Background

The DOE's Grid Modernization Laboratory Consortium (GMLC) Multi-Year Program Plan [2]

states, "…security and resilience of the modern electric grid may be defined as the functional preservation of the electric grid operations in the face of natural and man-made threats and hazards."

While the U.S. electric grid is highly reliable, severe weather events and cyber-attacks threaten to cause extensive damage to its aging infrastructure, resulting in extended periods of outage for customers. The economic impacts of weather-related outages in 2012 were estimated at between $27 and $52 billion [5]. Since 2000, the five-year average number of outages per year has doubled every five years, and the average number of monthly outages have increased six-fold [6].

The U.S. Energy Information Administration (EIA) defines industrial electricity customers as the "facilities and equipment used for producing, processing, or assembling goods" [7]. Industrial electricity customers make up 0.56% of electricity customers [8], but account for roughly 25% of all energy sales in the U.S. [9]. A single hour-long outage can cause the loss of hundreds of thousands to millions of dollars in output, lost inventory, brand degradation, and restart costs.

A microgrid, per DOE's terms [10], is: ''a group of interconnected loads and distributed energy resources within defined electrical boundaries that acts as a single controllable entity with respect to the grid. A microgrid can connect and disconnect from the grid to enable it to operate in both grid-connected or island mode.''

Microgrid research is constantly evolving to include advanced controls and communication systems for a wide range of applications [11] [12] [13] [14]. Capabilities enabled by microgrid technologies include: 1) seamless transition; 2) renewables integration; 3) voltage support; 4) peak shaving, 5) economic dispatch; 6) energy shifting; and 7) black start.

2.1. Case Study Environment

First-generation microgrids have focused primarily on priority critical loads, such as hospitals, military bases, and college campuses [15] [16] [17]. These types of facilities play vital roles to the country and are dependent on highly reliable power.

Similarly, many industrial facilities are critical to the daily operations of people and businesses across the country. The UPS Worldport facility is the largest automated package handling facility in the world [18] [19], processing approximately 416,000 packages per hour. As an air hub with more than 300 flights arriving and departing daily, Worldport has very strict requirements on flight schedules. Even a small electrical outage which stops the sorting equipment for a few minutes causes far-reaching ripples to those people and businesses depending on their service. Delays on time-critical packages such as refrigerated vaccines and living tissues could be disastrous to those depending on the materials.

UPS is a global leader in logistics, offering a broad range of solutions including transporting packages and freight; facilitating international trade, and deploying advanced technology to more efficiently manage the world of business. Headquartered in Atlanta, UPS serves more than 220 countries and territories worldwide. The facilities of interest include: Worldport, Centennial Hub, and SCS campus (though SCS data is not included in this analysis).

3. Process and Results

To understand how a microgrid bolsters resilience for a facility, it is critical to quantify the risks the facility faces daily and design to mitigate specific scenarios.

The All Hazards Econometrics System (AHES) is a Cybernomics computational method for determining Mean Failure Cost (MFC) [20] [21] [22], modified herein from Cyber Security Econometrics System (CSES) [3] [23] [24] used previously in industrial settings [25]; applied to industry standards [26] [27]; and applied to cloud environments [27] [28]. The cost/benefits risk assessment of the project [2] was carried out by computing the Mean Failure Cost (MFC) for various UPS stakeholders addressing grid vulnerability, consequence, and risk analysis. The reduction in MFC can then be matched against the costs and risks of deploying them, using relevant ROI functions.

3.1. Tools Used to Determine Mean Failure Cost

The value-based metric (MFC), when applied, quantifies the risks to an enterprise system on an individual stakeholder basis. MFC represents the loss that potentially results from threats and system vulnerabilities. MFC depends on the inherent system infrastructure (e.g., weaknesses) and accounts for the stakeholders' variances in terms of their individual mission requirements, that are satisfied via that infrastructure has in meeting each enterprise requirement.

3.2. Steps for Determining Mean Failure Cost

The essential steps involve I/O components and phases (i.e., discovery, classification and evaluation, metrics and mitigation as shown in Figure 1). The data collection/analysis consist of systems stakeholders, system specifications and requirements. System components makeup the requirements and the associated natural threats that exist. These natural

threats have the potential of causing a negative impact on the normal operations of the overall system. In this study, we address only rigorously documented natural hazards (i.e., threats) which cannot be altered (i.e., are immutable). The steps in determining MFC, when applied, result in the AHES method which was essentially derived as part of this case study.

To estimate the MFC for the set of stakeholders of a system, we identify and then maintain the following information: (1) the set of stakeholders; (2) the set of functional specifications/requirements; (3) for each stakeholder row and each requirement column, the stake that the stakeholder attaches to the selected service (or conversely, the cost that the stakeholder incurs if the service is disrupted (i.e., Stakes Matrix (ST)); and (4) for each component column of a specific requirement row (i.e., Dependency Matrix (DP)), the likelihood that the system provides that specific service requirement. The likelihood of a materialized threat column entries impacting the component row entries (i.e., Impact Matrix (IM)) is dependent on the probability of the emergence of a threat (i.e., Probability Threat vector (PT)) and the likelihood that such a threat would affect that component. The AHES method involves the generation of ST, DP, IM, as well as the PT. We derive the vector of mean failure costs (one entry per stakeholder) by Eq. (1) as a baseline:

$$MFC = ST \circ DP \circ IM \circ PT \quad (1)$$

3.3. IM Generation Using Mitigation Cost Estimates

Several studies in the past have used CSES to assess changes (i.e., Δ) resulting from mitigations (e.g., investments aimed at improving/hardening the infrastructures). The MFC formula [29] maps a threat configuration (PT) onto a vector of mean failure costs (MFC). When a security measure is deployed, its impact can be measured by considering how it affects the threat configuration (say, PT' instead of PT) and thereby how it affects (hopefully reduces) the MFC vector (MFC' instead of MFC). In [30], the ΔMFC was used as a measure of the effectiveness of security measures in hardening the infrastructure. This measure supported the following decisions.

First, stakeholders can determine whether a measure is worthwhile by matching its deployment cost against its benefit, represented in terms of the reduced MFC (and represented in monetary terms). The decision can, in fact, be modeled as a return on investment (ROI).

Second, analysts can also use the MFC reduction for each stakeholder as a basis for distributing the cost of the measure on the various system stakeholders. In [30], we discussed alternative ways to do this.

Third, managers can use the cost sharing formula to assess how much the measure costs them and use the MFC reductions to quantify their respective gains from the measure. Using this information, an ROI is computed. An ROI enables us to determine whether the measure benefits them individually. Previously documented approaches illustrated this premise [31].

For the sake of illustration, previously documented, consider the threat vector has been reduced to the new value: PT′. The gain in mean failure cost can then be estimated using the equation:

$$\Delta MFC = ST \circ DP \circ IM \circ \Delta PT \quad (2)$$

where $\Delta PT = PT' - PT$. This results in the gain in MFC in monetary units/time frame and shows the added value gained by stakeholders.

The following example illustrates how to judge the cost effectiveness of a given enhancement. For a given security enhancement measure, the service provider can determine the cost effectiveness by comparing the cost of installing the enhancement versus the gains in subscriber fees collected because of enhanced security (minus any subscriber loss that may result). This can be modeled as a ROI decision, as discussed in [30] and adapted from [22] [23].

Since we are only concerned about naturally occurring hazards (i.e., threats), which cannot necessarily be altered, we introduce a new concept for AHES that can be regulated. Natural hazards are normally assumed to occur based on historical evidence [32]. The effect of a materializing threat can however, be mitigated by improving/hardening the cyber/physical infrastructure. Moreover, the damage anticipated can be reduced if the enterprise environment is altered (i.e., harden the system) based on the risk informed assessment information. Thus, we introduce a new interpretation which results in a change from the baseline probability represented in IM from the baseline that Component C_k fails once threat T_q has materialized giving us IM′ or ΔIM.

The beneficial gain in mean failure cost (as expressed monetarily by the reduction in failure cost) can now be estimated as:

$$\Delta MFC = ST \circ DP \circ \Delta IM \circ PT \quad (3)$$

where $\Delta IM = IM' - IM$. This results in a positive gain overall for the MFC in monetary units/time frame (in our case $/day). This moreover, shows the added value (ROI) gained by stakeholders from an enhanced architecture. Equally, in our case, the analysis helps us understand the savings produced from hardening the

enterprise against natural threats and assists decision makers in commercial ROI decisions. The resulting AHES method (calculation of MFC) helps decision makers by putting a monetary value on the service that is delivered to stakeholders. In general, the stakeholders collectively perform the organizational mission requirements and therefore the overall benefactor is the organization or "enterprise" as discussed above.

Table 1. Collective UPS Facilities Specific Daily Monetary Failure Loss by Stakeholder*

Stakeholder	Volume Per Day (# of Packages)	Revenue per Package	Revenue per Day (Failure Cost)
Worldport	1,600,000	$18.86	$30,332,800
Centennial Hub – Current	640,000	$8.37	$5,356,800
Centennial Hub - Expansion	1,360,000	$8.37	$11,383,200

* Data calculated from UPS, Inc. second quarter earnings report ending June 30, 2017 [34].

3.4. Estimating ΔMFC – A Case in Point

In [32], Louisville Metro prepared its Hazard Mitigation Plan pursuant to the Section 322 of the Robert T. Stafford Disaster Relief and Emergency Assistance Act, 42 U.S.C. 5165, as amended by Section 104 of the Disaster Mitigation Act of 2000, P.L. 106-390 (DMA 2000) and regulations set forth in 44 CFR §201 [33]. The Plan identifies potential hazards, assesses risk, and presents mitigation strategies to build community resilience. The expected loss is reduced if we alter the enterprise environment (i.e., harden the system).

The beneficial gain in mean failure cost (as expressed monetarily by the reduction in failure cost) is thus estimated as shown in Eq. 3. In the analysis of the UPS Worldport and Centennial facilities at Louisville, Kentucky, we considered the unique stakeholders for the enterprise as the following: 1) UPS Facilities at Louisville – UPS Enterprise Stakeholders collectively; 2) UPS Facility – Worldport Stakeholders; and 3) UPS Facility – Centennial Hub Stakeholders. The individual contribution of the respective stakeholders is documented in Table 1.

The collective UPS Enterprise Stakeholders at the Louisville complex versus their respective requirements can be depicted as the Stakes Matrix (ST) Table 2. The logic for the ST depends on the following premises: (1) a stakeholder may have different stakes in different requirements; and (2) a functional requirement may carry different stakes for different stakeholders. The best way to represent this situation is through a two-dimensional matrix, where the rows represent stakeholders, the columns represent operational requirements and the entries represent stakes, as shown in Table 2.

The failure cost in each column's cell in Table 2 is the monetary amount for the respective stakeholder (the row entry) when the system fails to meet each stakeholder's functional requirement. We therefore quantify theses variables in terms of financial loss per unit of operation time (e.g., $/day); it represents the mean loss that the stakeholder may experience in case of a failure.

Table 1 represents the potential monetary loss by a stakeholder. The analysis team worked closely with UPS participants to determine the best and most accurate data to populate the AHES matrices. Data was analyzed from the UPS, Inc. second quarter earnings report ending June 30, 2017, and was used to calculate the Worldport and Centennial Hub stakeholder's monetary loss [34]. The following logic was used to determine the Worldport and Centennial Hub, stakeholder's mean financial loss:

Worldport - From the 2017 second quarter earnings report [34], the per package revenue is calculated as a weighted combination of two revenues: the next day delivery cost and the international package cost. The revenue per package is comprised from 80% of the next day delivery sort revenue ($19.62 per package) plus

Table 2. Collective UPS Facilities Stakes (ST) Matrix: Populated UPS Stakeholders versus UPS Louisville Facility Requirements*

Stakes (ST)		Requirements		
		Worldport Availability	Centennial (Expansion) Availability	No Req't. Failure (NRF)
Stakeholders	UPS Enterprise Collectively	$30,583,000	$11,380,000	$0
	Worldport	$30,332,000	$0	$0
	Centennial Hub (Current)	$0	$5,356,800	$0
	Centennial Hub (Expansion)	$0	$11,383,200	$0

* Source data derived from UPS, Inc. 2017 second quarter earnings report [34] and from [35].

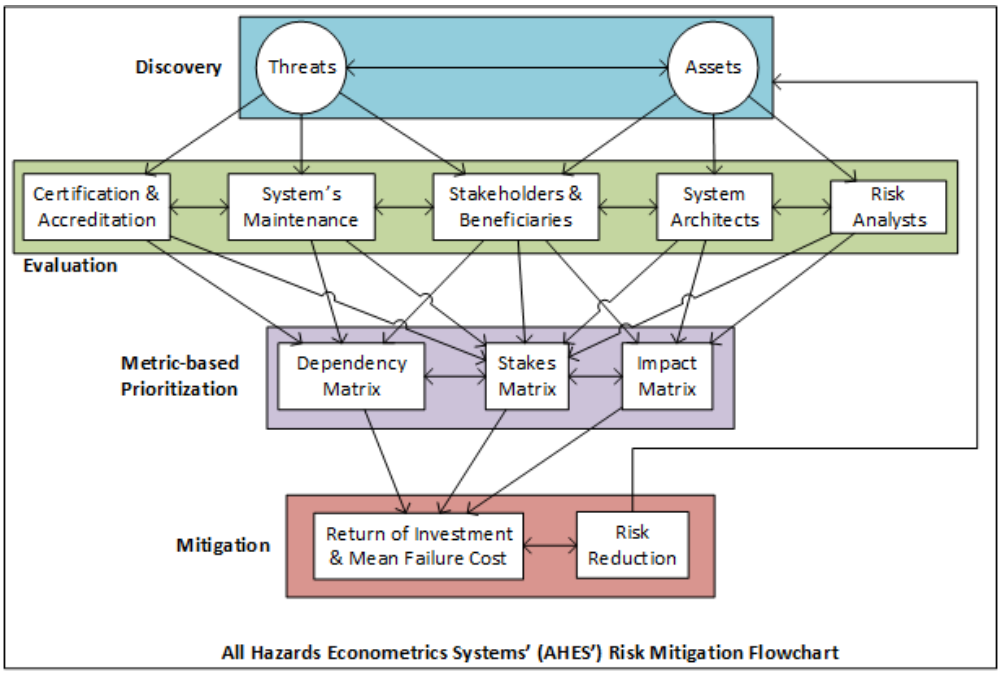

Figure 2: AHES' Risk Mitigation Flowchart

20% from the total international package revenue ($16.31 per package).

Centennial Hub "Current" – The Centennial Hub building first opened in May of 2008, with a sorting capacity of 40,000 packages per hour. That translates in 640,000 packages per day (two eight-hour shifts). From the 2017 second quarter earnings report [34], the per package revenue for U.S. Domestic package ground ($8.37) is herein used for calculating the specific daily revenue per Day Failure Cost.

Centennial Hub "Expansion" – The expansion of enhanced technology in the Centennial Hub facility will increase capacity to 85,000 packages per hour, improving both reliability and quality of service provided to UPS customers [35]. The UPS Centennial Hub will triple the size of the current package sorting facility to 838,000 square feet, and nearly double its current sorting capacity to 85,000 packages per hour [36] which results in 1,3600,00 packages per day (two eight-hour shifts). From the 2017 second quarter earnings report [34], the per package revenue for U.S.

Table 3. Collective UPS Facilities Dependency (DP) Matrix

Dependency (DP)		Components								
		Electricity Distribution	Electric Grid Infrastructure	Installation Unique Sorting Equipment	Computers	Lighting	Air Conditioning Equipment	Airplanes Functioning & on time	Truck Support Vehicles Functioning	NCF
Requirements	Fuel Farm Availability	0.2	0.2	0	0.2	0.1	0.0	0	0.3	0
	World Port Availability	0.2	0.2	0.1	0.2	0.1	0.2	0	0	0
	Centennial Availability	0.2	0.2	0.15	0.2	0.08	0.07	0	0.1	0
	NRF	0.4	0.4	0.75	0.4	0.72	0.73	1	6	1

Note: The NRF row represents the case when a component fails but does not affect the associated requirement. The NCF column represents the case when no component fails.

Table 4. Collective UPS Facilities Impact (IM) Matrix

Impact (IM)		Threats									
		Flooding	Severe Thunder storms	Hailstorms	Tornado	Earthquake	Severe Winter Storms	Dam Failure / Sinkholes / Landslides	Extreme Heat / Drought	Fires / Chemical Spills	No Threats
Components	Electricity Distribution	0.3	0.3	0.04	0.14	0.125	0.1	0.125	0.2	0.1	0
	Electric Grid Infrastructure	0.3	0.3	0.04	0.14	0.125	0.1	0.125	0.2	0.1	0
	Installation Unique Sorting Equipment	0	0.01	0.04	0.1	0.125	0.15	0.125	0	0.1	0
	Computers	0.1	0.2	0.04	0.1	0.125	0.05	0.125	0.15	0.1	0
	Lighting	0.1	0.02	0.04	0.1	0.125	0.1	0.125	0.15	0.1	0
	Air Conditioning Equipment	0.1	0.02	0.2	0.14	0.125	0.1	0.125	0.3	0.1	0
	Airplanes - Functioning & On time	0	0.1	0.3	0.14	0.125	0.1	0.125	0	0.2	0
	Trucks & Support Vehicles Functioning	0.1	0.05	0.3	0.14	0.125	0.1	0.125	0	0.2	0
	No Component Failure	0	0	0	0	0	0	0	0	0	1

Note: the NCF row represents the case when a threat materializes but does not affect the associated component. The No Threat column represents the case when no threat materializes.

Domestic package ground ($8.37) is herein used for calculating the specific daily revenue per Day Failure Cost.

Natural hazards were evaluated. We considered the dependency of the stakeholders' requirement of availability as key to fulfilling the respective stakeholders' individual and collective requirements with regards to their missions.

The respective components to the stakeholder's requirements of availability included: 1) Electricity Distribution; 2) Electric Grid Infrastructure; 3) Installation Unique Sorting Equipment; 4) Computers; 5) Lighting; 6) Air Conditioning Equipment; 7) Airplanes Functioning & on time Truck Support Vehicles Functioning; and 8) No Component Failure (NCF). The probability of the system failing, with respect to a given requirement and given that a component has failed, is shown in Table 3.

UPS, Inc. stated in an annual report on Form 10-K [37], filed with the U.S. Securities and Exchange Commission, the following.: **"Severe weather or other natural or manmade disasters could adversely affect our business."**

Components of the UPS enterprise architecture of the facilities at the Louisville complex may fail to operate properly because of functional breakdowns

Table 5. Probability Threat (PT) Vector*

Probability Threat (PT) Vector		Probability of threat materializing
Threats	Flooding	0.3479
	Severe Thunderstorms	0.0285
	Hailstorms	0.0077
	Tornado	0.0012
	Earthquake	0.0003
	Severe Winter Storms	0.0174
	Dam Failure/Sinkholes / Landslides	0.0025
	Extreme Heat/Drought	0.0099
	Fires/Chemical Spills	0.3235
	Other Threats – Man-Made – Outside Scope	0.2598
	No Threats	0
	All Threats	0.9990

* Calculated from Louisville Metro Hazard Mitigation Plan "Loss Matrix" table in [32].

brought about by natural hazards or man-made hazardous activity. To continue the analysis, the natural hazards that threaten the facilities were cataloged, in the same way that analysts of a system's reliability define a fault model. We used the catalog of threats that were established in the 2016 Louisville Metro Hazard Mitigation Plan (updated every five years) [32], and the Kentucky Emergency Operations Plan (KYEOP) [38] modeled after the guidance provided by Department of Homeland Security and FEMA [39]. The entities in Kentucky all-hazards emergency plan are required by Kentucky Revised Statue (KRS) 39A [40] and is activated upon order of the Governor of the Commonwealth of Kentucky [38].

Due to Louisville's geology, climate, and geographical setting, the metro area is vulnerable to a wide array of natural hazards that threaten life and property. The Louisville Metro Hazard Profiles catalogs the hazards, which were previously identified as affecting the Louisville Metro Area. These Profiles were created using the best available data from a variety of resources, including: the National Centers for Environmental Information (NCEI), formerly the National Climatic Data Center (NCDC), National Weather Service (NWS), Louisville/Jefferson County Information Consortium (LOJIC), Corps of Engineers: Louisville District, Kentucky Office of Geographical Information, Kentucky Geological Survey (KGS), Kentucky State Climatology Center, Midwestern Regional Climate Center (MRCC), FEMA Hazard Mapping website, local agencies and newspaper articles, previous Local Hazard Mitigation Plan's, the approved 2013 Kentucky Enhanced State Hazard Mitigation Plan [41], and the 2014 Kentucky Operations Plan [38].

Through research of historic impacts, occurrences, dollar losses to date, review of the past State and Local Hazard Mitigation Plans and discussions with key agencies and stakeholders, the following thirteen (13) hazards are assessed in the 2016 Louisville Metro Hazard Mitigation Plan [32]: (1-2) Flood Related Hazards (Flood, Dam/Levee Failure, (3-6) Meteorological Hazards (Tornado, Severe Winter Storm, Severe Storm, Hailstorm), (7-9) Geologic Hazards (Earthquake, Landslide, Karst/Sinkhole), (10-13) Other Hazard Types (Hazardous Materials, Drought, Extreme Heat, Fires/Chemical Spills).

Understanding the documented risk and each hazard is critical to determining the impact on the UPS Louisville facilities. The record for the number of weather and climate disasters that exceeded $1 billion (U.S. dollars) in losses was set in 2011 [42] [43] [44]. This data may be usurped by recent data concerning Hurricane Harvey and its cumulative effects in 2017. The above threats are cataloged in Table 4 and their respective impacts are populated in Table 4.

Table 6. Collective UPS Facilities Mean Failure Cost (MFC) per day in USD*

Stakeholders	MFC Baseline	MFC 50% Reduced Sort	MFC 99% Energy Availability
UPS Enterprise - Collectively	$4,418,054	$3,768,523	$1,820,570
Worldport	$3,085,953	$2,627,759	$1,253,626
Centennial Hub (Current)	$557,887	$477,631	$236,942
Centennial Hub (Expansion)	$1,185,511	$1,014,966	$503,502

* AHES) is a Cybernomics computational method for determining MFC [20] [21] [22], modified herein from CSES [3] [23] [24].

The "Loss Matrix" table in [32] provided quantitative data that portrays which hazards have the potential to cause the most devastation, based on frequencies and damage numbers, where available. The data was used by the project team to help prioritize which hazards should receive the most consideration when justifying potential mitigation projects in current specific efforts regarding the placement and the configuration of the microgrid and its analysis. It was the intent of this effort that other commercial entities, including UPS, will use this technique in the future. The loss and occurrence data (based on the number of events divided by the total number of damages) was used to populate the threat probability vector (Table 5), which is used in calculating MFC. As mentioned [32], this data can be improved and Louisville Metro is dedicated to keeping better loss information to improve the results of this model.

Given the populated stakes matrix ST, the dependency matrix DP, the impact matrix IM and the threat vector PT, we now can derive the MFC by Eq. 1. The resultant MFC for the UPS enterprise at the Louisville facility is represented as the MFC per stakeholder in Table 6.

During the course of this study, a reduced sort (50%) solution addressed a way to allow the advantages of the microgrid to be evaluated in the context of risk assessment [45]. The cumulative amount of power by implementing the microgrid solution is also approximately 50% of the needed power to run the facility. Secondly, the SNL MDT model quantified the energy availability (99%) by adding generator capacity to UPS's microgrid. From this data, we reduced from the baseline: the component "Electric Grid Infrastructure" row in the IM (Table 4) by 50%; and the rows, "Electric Distribution", and "Electric Grid

Infrastructure" (Table 4) by 99%. Table 6 identifies the baseline MFC for the specified stakeholders and the per cent reduction in MFC by hardening the environment by percentage amounts of 50% reduced sort and 99%. energy availability.

4. Conclusions

The reduction in MFC (as expressed in USD/day) was derived by applying Eq. 2. This shows the added value gained by each stakeholder due to a more resilient COOP architecture (i.e., hardening the enterprise against natural hazardous threats). The analysis provided a basis for prepositioning backup generation capacity, and enhancements that promise cost savings and ROI. In this way the AHES method helps decision makers better understand the value of the service and that is delivered to stakeholders enabling mission requirements. These numbers are directly comparable and give a bottom line understanding of the potential impact, root cause (i.e., source) that includes the kill chain from threat to asset and the affect to operations and in all stakeholders.

The beneficial impact to the collective UPS Facilities is shown in Table 6. This is achieved by implementing the various components of the microgrid solutions. The MFC reduction ranges from 14-15% for the 50% Reduced Sort and from 56-59% for the 99% Energy Availability. Based on AHES's MFC, the best microgrid implementation that UPS should consider for their particular facilities' implementation, has been reduced to a business decision. The AHES method provides the logic to "grade" the level of ROI (a graded approach) desired for this business decision. This paper considers the industrial viewpoint and uses real world data for COOP planning.

This work was supported by a grant from DOE. We derived the AHES methodology from CSES (as the basis) to track many facets of the cause/loss-impact to operations. In this way, COOP planners determined the primary operational weaknesses and could prioritize course of action based on the cost of mitigation (i.e., hardening solutions) and the prospect of ROI. The artifacts of this investigation will be useful on an ongoing basis for assessment and risk abatement.

5. References

[1] Z. Cheng, J. Duan and M.-Y. Chow, "To Centratlize or to Distribute: That is the Question - A Comparison of Advanced Management Systems," IEEE Industrial Electronics Magazine, pp. 6-24, 21 March 2018.

[2] Department of Energy Grid Modernization Initiative (GMI), "DOE Grid Modernization Laboratory Consortium (GMLC) - Awards," 2016. [Online]. Available: https://energy.gov/under-secretary-science-and-energy/doe-grid-modernization-laboratory-consortium-gmlc-awards. [Accessed 11 June 2018].

[3] R. K. Abercrombie, F. T. Sheldon and E. M. Ferragut, "Cyberspace Security System". United States Patent 8,762,188, 24 June 2014.

[4] Sandia National Laboratories, "The Microgrid Design Toolkit," U.S. Department of Energy, Energy Efficiency & Renewable Energy, 24 March 2017. [Online]. Available: http://techportal.eere.energy.gov/technology.do/techID=1468. [Accessed 11 June 2018].

[5] Department of Energy, "Economic Benefits of Increasing Electric Grid Resilience to Weather Outages," 2013. [Online]. Available: https://energy.gov/downloads/economic-benefits-increasing-electric-grid-resilience-weather-outages. [Accessed 11 June 2018].

[6] J. Wirs-Brock, "Power Outages on the Rise across the U.S.," Inside Energy, 18 August 2014.

[7] U.S. Energy Information Administration, "U.S. Energy Information Administration Glossary," 2018. [Online]. Available: https://www.eia.gov/tools/glossary/index.php?id=I. [Accessed 11 June 2018].

[8] U.S. Energy Information Administration, "Electricity - Detailed State Data," 9 March 2018. [Online]. Available: https://www.eia.gov/electricity/data/state/. [Accessed 11 June 2018].

[9] U.S. Energy Information Administration, "Short-Term Energy Outlook September 2017," U.S. Department of Energy, Washington, DC, 2017.

[10] D. T. Ton and M. A. Smith, "The U.S. Department of Energy's Microgrid Initiative," The Electricity Journal, vol. 25, no. 8, pp. 84-94, October 2012.

[11] M. Stark, A. Herron, D. King and X. Xue, "Implementation of a Publish-Subscribe Protocol in Microgrid Islanding and Resynchronization with Self-Discovery," IEEE Transactions on Smart Grid, vol. PP, no. 99, pp. 1-1, 2017.

[12] B. Ollis, P. Irminger, M. Buckner, I. Ray, D. King, A. Herron, B. Xiao, R. Borges, M. Starke, Y. Xue and B. Maccleery, "Software-defined intelligent grid research integration and development platform," in 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Minneapolis, MN, 2016.

[13] M. Starke, B. Xiao, G. Liu, B. Ollis, P. Irminger, D. King, A. Herron and Y. Xue, "Architecture and implementation of microgrid controller," in 2016 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT), Minneapolis, MN, 2016.

[14] G. Liu, M. Starke, B. Xiao and K. Tomsov, "Robust optimisation-based microgrid scheduling with islanding constraints," IET Generation, Transmission & Distribution, vol. 11, no. 7, pp. 1820-1828, 2017.

[15] P. Stluka, D. Godbole and T. Samad, "Energy management for buildings and microgrids," in 2011 50th IEEE Conference on Decision and Control and European Control Conference (CDC-ECC), Orlando, FL, 2011.

[16] A. G. Skowronska-Kurec, S. T. Eick and E. T. Kallio, "Demonstration of Microgrid technology at a military installation," in 2012 IEEE Power and Energy Society General Meeting, San Diego, CA, 2012.

[17] T. Ersal, C. Ahn, I. A. Hiskens, H. Peng and J. L. Stein, "Impact of controlled plug-in EVs on microgrids: A military

microgrid example," in 2011 IEEE Power and Energy Society General Meeting, San Diego, CA, 2011.
[18] United Parcel Service, "UPS Worldport Fact Sheet - 2017," United Parcel Service and America, Inc., 2018. [Online]. Available: https://www.pressroom.ups.com/assets/pdf/pressroom/fact%20sheet/Worldport%20Fact%20Sheet-2017.pdf. [Accessed 11 June 2018].
[19] A. Dean, "Photo Essay: UPS Worldport," 25 June 2015. [Online]. Available: https://www.manufacturing.net/news/2015/06/photo-essay-ups-worldport. [Accessed 11 June 2018].
[20] A. Mili and F. T. Sheldon, "Measuring Reliability as a Mean Failure Cost," in 10th IEEE High Assurance Systems Engineering Symposium (HASE '07), Plano, TX, 2007.
[21] A. Mili and F. T. Sheldon, "Challenging the Mean Time to Failure: Measuring Dependability as a Mean Failure Cost," in 42nd Hawaii International Conference on System Sciences (HICSS '09), Big Island, HI, USA, 2009.
[22] F. T. Sheldon, R. K. Abercrombie and A. Mili, "Methodology for Evaluating Security Controls Based on Key Performance Indicators and Stakeholder Mission," in 42nd Hawaii International Conference on System Sciences (HICSS '09), Big Island, HI, USA, 2009.
[23] R. K. Abercrombie, B. G. Schlicher, F. T. Sheldon, M. W. Lantz and K. R. Hauser, Cyberspace Security Econometrics Systems (CSES), U.S. Copyright TxU 1-901-039, Washington, DC: US Library of Congress, 2014.
[24] R. K. Abercrombie, "Cyptographic Key Management and Critical Risk Assessment (ORNL/TM-2014/131)," Oak Ridge National Laboratory, Oak Ridge, TN, 2014.
[25] Q. Chen, R. K. Abercrombie and F. T. Sheldon, "Risk Assessment for Industrial Control Systems - Quantifying Availability Using Mean Failure Cost (MFC)," Journal of Artificial Intelligence and Soft Computing Research, vol. 5, no. 3, pp. 205-220, September 2015.
[26] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantz and A. Mili, "Risk Assessment Methodology Based on the NISTIR 7628 Guidelines," in 2013 46th Hawaii International Conference on System Sciences (HICSS-46), Wailea, Maui, Hawaii, 2013.
[27] A. A. Jillepalli, D. Conte de Leon, M. Haney, F. T. Sheldon and R. K. Abercrombie, "Security Management of Cyber-Physical Control Systems Using NIST SP-800-82r2," in 13th International Wireless Communications and Mobile Computing Conference (IWCMC-2017), Valencia, Spain, 2017.
[28] N. M. Ahmed, "Measuring Cloud Security Risk by Mean Failure Cost," in 2016 IEEE Symposium Series on Computational Intelligence (SSCI), Athens, Greece, 2016.
[29] A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon and A. Mili, "Defining and computing a value based cyber-security measure," Information Systems and e-Business Management, vol. 10, no. 4, pp. 433-453, 2012.
[30] A. Ben Aissa, R. K. Abercrombie, F. T. Sheldon and A. Mili, "Quantifying Security Threats and Their Potential Impacts: A Case Study," Innovations in Systems and Software Engineering, vol. 6, pp. 269-281, 2010.
[31] L. B. A. Rabai, M. Jouini, A. Ben Aissa and A. Mili, "A Cybersecurity Model in Cloud Computing Environments," Journal of King Saud University – Computer and Information Sciences, vol. 25, no. 1, pp. 63-75, 2013.
[32] Louisville Metro Council, "2016 Louisville Metro Hazard Mitigation Plan," Louisville, KY, 2016.
[33] Federal Emergency Management Agency, Department of Homeland Security, "44 CFR 201.6 - Local Mitigation Plans," Code of Federal Regulations, Washington, DC, 2013.
[34] United Parcel Service, Inc., "United Parcel Service, Inc. Selected Financial Data - Second Quarter 2017 Earnings Report," 2017. [Online]. Available: https://pressroom.ups.com/assets/pdf/pressroom/fact%20sheet/2017_2Q_Earnings_Tables.pdf. [Accessed 13 June 2018].
[35] M. Polk, "UPS Breaks Ground on Louisville Centennial Hub Expansion," GlobeNewswire, 25 August 2016. [Online]. Available: https://globenewswire.com/news-release/2016/08/25/866943/0/en/UPS-Breaks-Ground-on-Louisville-Centennial-Hub-Expansion.html. [Accessed 13 June 2018].
[36] C. Kelsch, "UPS – Centennial Hub Expansion," 31 May 2017. [Online]. Available: http://www.construction-today.com/sections/commercial/3092-ups-centennial-hub-expansion. [Accessed 13 June 2018].
[37] United Parcel Service, Inc., "Annual Report Pursuant to Section 13 or 15(d) of the Securities Exchange Act of 1934," 31 December 2012. [Online]. Available: https://www.sec.gov/Archives/edgar/data/1090727/000109072713000005/ups-12312012x10k.htm. [Accessed 13 June 2018].
[38] Kentucky Emergency Management, "Kentucky Operations Plan," Commonwealth of Kentucky, 2014.
[39] Federal Emergency Management Agency, Department of Homeland Security, "Hazard Mitigation Planning and Hazard Mitigation Grant Program," Federal Register, Vol. 67, No. 38, Tuesday, February 26, 2002, Washington, DC, 2002.
[40] Kentucky Legislature, "Kentucky Legislature - Kentucky Revise Statues (KRS) Chapter 39A," KRS Database, 11 June 2018. [Online]. Available: http://www.lrc.ky.gov/statutes/chapter.aspx?id=37202. [Accessed 13 June 2018].
[41] Kentucky Emergency Management (KYEM), "Commonwealth of Kentucky Enhanced Hazard Mitigation Plan - 2013 Version," Kentucky Emergency Management (KYEM), Frankfort, KY, 2013.
[42] K. Kunkel, T. R. Karl and H. Brooks, "Monitoring and Understanding Trends in Extreme Storms - State of Knowledge," Bulletin of the American Meteorological Society, vol. 51, pp. 499-514, 2013.
[43] "Billion-Dollar Weather and Climate Disasters," NOAA National Centers for Environmental Information (NCEI), 6 April 2018. [Online]. Available: https://www.ncdc.noaa.gov/billions/events/US/1980-2017. [Accessed 13 June 2018].
[44] "Billion-Dollar Weather and Climate Disasters: Summary Stats (2018)," NOAA National Centers for Environmental Information (NCEI), 6 April 2018. [Online]. Available: https://www.ncdc.noaa.gov/billions/summary-stats. [Accessed 13 June 2018].
[45] B. Ollis, N. Stenvig, R. K. Abercrombie, B. Xiao, J. Storey, M. Bhandari, B. Schenkman, M. Baca, J. Eddy and A. Wachtel, "Industrial Microgrid Design and Analysis for Energy Security and Resiliency," ORNL/LTR-2017/480, 2017.