# Homeland Defense & Security Information Analysis Center
# Technical Inquiry Response Report

## *Attributing (Negative) Value to Electricity System Outages at Military Installations*

**Thursday, June 18, 2020**

**IN RESPONSE TO:**

**A Technical Inquiry submitted by Office of the Deputy Assistant Secretary of the Army for Energy & Sustainability [ODASA(E&S)]**

**PREPARED FOR:**

**Dr. Bret Strogen, Special Assistant for Energy & Sustainability, Office of the Assistant Secretary of the Army for Energy, Installations & Environment**


**PREPARED BY: Cully A. Patch HDIAC Analyst; cpatch@hdiac.org**
**APPROVED BY: Steve Redifer, HDIAC Director; sredifer@hdiac.org**

HDIAC Homeland Defense & Security Information Analysis Center
*Operated by*
*Quanterion Solutions Incorporated*

901 N. Stuart Street
Suite 401
Arlington, VA 22203

www.hdiac.org
info@hdiac.org

# HDIAC Technical Inquiry Response

## Attributing (Negative) Value to Electricity System Outages at Military Installations

## 1. Inquiry

HDIAC received the following technical inquiry from the Special Assistant for Energy & Sustainability, Headquarters, Department of the Army, Dr. Bret Strogen:

"I would like assistance coming up with a conservative approach to attribute (negative) value to electricity system outages at military installations. (Eventually, I may want to expand the scope to natural gas, water, and even access to training ranges.)
Industrial facilities can estimate profit loss per hour when factories/machines/servers are down for maintenance or workers are unavailable (due to strikes, illness, etc.).
The DoD is certainly not analogous to a commercial factory, but what can we learn from existing studies, to help us value (and therefore help justify dedication of resources) upgrading and maintaining our electricity systems (to improve reliability)? What literature is out there that could inform such decisions?
In a quick (definitely not exhaustive) Google Scholar search, I found the following articles that--given titles alone--sound relevant.
- Cost-benefit analysis of emergency backup power systems for mission critical applications
- Valuing Energy Security: Customer Damage Function Methodology and Case Studies at DoD Installations
- Multi-objective Value Analysis of Army Basic Training [1]."

**Customer Coordination:**

11 Jun – Initial contact via phone to discuss the tech inquiry to ensure HDIAC was in sync with Dr. Strogen's intentions. HDIAC provided initial thoughts and Dr. Strogen provided feedback as well as additional information sources to reference.

15 Jun – Dr. Strogen provided feedback on HDIAC proposed literature research as well as the need to provide quantitative ideas/approaches to some of the qualitative ideas offered.

# 2. HDIAC Response

Methodology. After consulting directly with Dr. Strogen on the requirements of the task, the HDIAC analyst used literature research to provide data regarding how to measure impact to DoD installations during subsequent utility outages. Based on the inquiry, the HDIAC analyst used operational experience as both a prior military watch officer as well as an intelligence planner for the Joint Task Force Civil Support to perform the research.

Sources. The HDIAC analyst undertook a literature review using resources found in the Defense Technical Information Center (DTIC) Research & Engineering (R&E) Gateway, as well as publicly available data, the results of which are provided in this report.

# 3. Background

## 3.1 Environment Definition

### *3.1.1 An Evolving, Multi-Generational, Yet, Still Mostly Centralized, Infrastructure*

As overall reliability of the electrical power supply environment has improved over the years, bulk-commercial energy is still delivered through a centralized generation, transmission, and distribution system. Once arriving to a DoD installation, through feeds from the local provider/authority, power is distributed throughout the installation using a Government-Owned, Government-Operated (GOGO), Government-Owned, Contractor-Operated (GOCO), or, most recently, a completely privatized model where the provider will both own and operate the on-installation power system. Through evolution of ever-increasing mission requirements bases, have developed different configurations, vendors, and technical refresh cycles that often combine several generations of equipment working together for operations, with much of this increasingly automated and controlled through a remote cyber-physical network.

At the loss of those feeds, centralized (albeit, likely multi-feeder sourced) power will be lost and all or part of the installation will run on their pre-planned Continuity of Operations (COOP)/developed power contingency plans until restoration. This starts the clock on available sustainment capacity which is limited to the established reserves based on both mission and/or DoD standards [2]. Depending on priority, this can range from banks of major power generators, uninterruptable power supplies (UPS), and storage capacity of multiple buildings or each building, to backup batteries of operator endpoint devices. These pockets and scales of backup equipment, though fairly coordinated by site, building or individual, are not normally connected/coordinated site-to-site across the installation in

terms of understanding individual energy generation, distribution, and storage, nor can they readily share these resources.

### *3.1.2 A Demonstrated and Evolving Distributed Smart Microgrid Infrastructure*

Due to recent investment in renewable energy and distributed microgrid technology in the form of pilot programs and Joint Capability Technology Demonstrations (JCTDs) (e.g. Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS)), a limited number of bases have created microgrid environments that produce, transmit, and distribute power within a very small portion of the base down to an individual building, and/or operator mobile equipment, to perform the mission. This equipment is increasingly coordinated and controlled through a secure cloud architecture that models modern albeit developing smart city technologies while increasing sensor and control technology to better manage generation, distribution, and consumption requirements. The advent of this technology, however, not only increases the cost and complexity of electrical energy operations, but also increases vulnerability footprints in the cyber-physical domain.

## 3.2 Problem Definition

**Given the environment above, what conservative approaches attribute (negative) value to electricity system outages at military installations?**

In order to help define the definition of negative value to electricity system outages at military installations below, it helps to tease out what "ends" are produced by an installation overall.

From the DoD standpoint, one would argue that this is associated with trying to measure an installation's Mission Assurance.

**The DoD defines Mission Assurance as:**

> "A process to protect or ensure the continued function and resilience of capabilities and assets—including personnel, equipment, facilities, networks, information and information systems, infrastructure, and supply chains—critical to the performance of DoD [mission-essential functions] in any operating environment or condition" [3].

Helping to define the issue from an energy standpoint, the Air Force has used the term **"Energy Assurance"** in a Rand Project Air Force (PAF) document as follows:

> "The purpose of this work is to develop a process for examining (and ultimately improving) the ability of Air Force installations and ground-based mission functions to support mission assurance by ensuring the continued function and resilience of capabilities and assets that depend on energy (in the form of electric power), in any operating environment or condition. We believe the term energy assurance best describes this overarching concept…" [4].

Lastly, the DoD definition of **Energy Resilience** aids in rounding out the overall focus:

> "DoD energy resilience is the ability to prepare for and recover from energy disruptions that impact mission assurance on military installations. ...DoD Installation Energy Resilience is both technology and authority agnostic. It is about mission and economic performance" [5].

The most prevalent definition of the problem was assessed to be the following: The traditional, mostly prevalent, and centralized infrastructure is generally decades old and lacks the specific information systems to adequately correlate energy loss with quantitative operational loss, especially in near-real time.

## 3.3 How to Measure Negative Impact of Energy Outages

### *3.3.1 Qualitative Measures*

The following is a thought exercise of the kinds of support an installation provides in order to identify the capabilities, importance, and priorities of those capabilities to support Mission Assurance.

**How do we measure outage Impact?**

**If based on cost, what is the definition of cost?**

People, Mission, Money, etc. - Money or other cost, as a means, tend to be more a quantitative measurement, but the ends are the most important but tend to be harder to measure. However, as identified by Dr. Strogen, because of the missions stated above, DoD Installations do not follow the more quantitative, profit-related measurements to show overall effectiveness, but what does?

One could argue that the People and the Mission are most important because they are the main reason the installation exists, but create challenges in measuring success or failure.

Measuring Negative Value/Impact - Government installations provide key security capabilities that contribute to overall stability, etc. This security and stability capability is also often more qualified than quantified, which requires a thought exercise on the "What" and "Why" a certain facility (or capability) exists in order to get to "How" negative value/impacts can be measured.

Possible Metrics (both qualitative and quantitative) include:

Mission Impact (time and space priority weighted)

- **Mission Dependency** - This could also include technical, communications and/or life support people in the immediate area, or dependent forces around the world (downstream effects)
- **Mission Timing** – Often used in combat, mission timing is critical as energy losses could literally range from zero impact to severe mission impact.
- **Presence of Backup Utility Capacity** – This can be estimated quantitatively, but is subject to many variables such as shutdown/shedding priority availability and sequencing to include the amount of automation of such decisions
    - e.g. **Mission and Physical Influences** – It will be likely necessary to shut down certain capabilities in a prioritized manner as capacity and time run out
- **Amount of Backup** – This is relatively the same as the presence of backup utility capacity (perhaps can cluster together as it is further considered)
- **Cognitive Influences** – The fact that one knows that he/she is using emergency systems and the resulting uncertainty (i.e. the fog of war, etc.) can have a significant effect on the best contingency plans
- **Additional Commercial Costs** - Off-hours responses, especially of unique specialists are required, as well as engineering tradeoffs of replacing or maintaining legacy systems

### *3.3.2 Quantitative Measurement Approaches*

Challenges. The need to help understand qualitative data quantitatively is no new task, especially if that qualitative data represents a significant threat. Terrorism and cyberattacks are two examples that are much more qualitative in nature than quantitative due to their relative low number and/or high variability of incidents. This problem set has been addressed by the Risk Management community for many years with varying results.

National Institute of Standards and Technology (NIST) Cybersecurity Framework Model. Some methods, such as the current Risk Management Framework (RMF) model, though not quantitative, involve definition-oriented, qualitative data to inform subject matter expert

(SME) consensus, which results in values to include rating on a discrete scale from non-applicable, to limited, moderate, and significant [6].

Department of Defense Cybersecurity Architecture Review (DODCAR) Model. Another non-quantitative, but illustrative, analysis that could adequately bridge the gap, the DODCAR Model consists of using an advanced persistent threat (APT), cybersecurity threat framework (in this case MITRE ATT&CK) as a standard overlay to score those threats against related cybersecurity capabilities. This results in a color-coded representation of the status of the attack surface that is not only easy to understand by decision makers, but also uses a heuristic algorithm to provide weighted scoring based on priority. Using the same overlay to note the prevalence of the same threats in the environment ultimately adds to provide both visual and quantitative indicators as to which threats to address first for maximum gains at minimum cost. For example, this system was used by the DoD in years past to determine that spending tens of millions of dollars on upgrading their enterprise IT operating system was ultimately more effective than spending hundreds of millions of dollars upgrading existing cybersecurity technology [7].

Quantification Through Confidence Interval Calibration. Some promising pseudo-quantitative data that is showing effectiveness in industry involves combining Bayesian patterns with training SMEs to reason and estimate quantitative answers to required questions for key measurements of success to a 90% confidence interval. Once this "calibration" training is completed, these values can be collected either through a consensus model or, to help minimize cognitive biases such as Group Think, can be individually collected, and then the values averaged. Once these values have been collected, analysts run standard Monte Carlo simulations with them, providing numerical data that can be used for evaluation and decision support [4].

# 4. Analysis

Overall. HDIAC analysis revealed large, centrally powered infrastructure presents a myriad of challenges due mostly to the lack of relationship data between the power generation, transmission, and especially, distribution, to the resulting negative impact value, both qualitative and quantitative, to installations measured from the proposed Mission and Energy Assurance definition. This generally introduces an unacceptable range gap for effective decision support on ways forward. However, with increased use of distributed micro-grid technology, combined with the sensor/actuator technology and secure cloud processing and storage, this not only allows increased resolution of these relationships, it creates an operating environment that can adapt generation, distribution, and consumption dynamically at priorities in both space and time to meet individual mission needs and dependencies.

Resulting Resiliency Measurement Considerations. This is resulting in a transformation from a whole installation with relatively few, select, unconnected backups, to series of self-contained, but mutually supporting, microgrids within the installation that add to the survivability and resiliency of an installation, while also complying with current and future Green Energy requirements and standards.

# 5. Conclusions

The traditional, prevalent, and centralized infrastructure is generally decades old and lacks the specific information systems to adequately correlate energy loss with quantitative operational loss, especially in near-real time. However, based on research of both literature and SME knowledge, HDIAC walked through a thought exercise of the current environment. This not only teased out the problem set and potential measurement approaches, but also made the best attempts to understand and approach the relationship between installation energy outages and impacts to the operational missions they support. This qualitative data along with qualitative to quantitative conversion models (used in other fields such as cybersecurity) are presented.

The likely future of energy supply will be a privatized, smart microgrid infrastructure that is promising to not only distributed energy supply and dependency/backup (hence resilience), but because of the increase of quantitative, data-driven management systems, there is a high probably of a reliable correlation with energy loss and mission impact to provide the best decision support.

Therefore, consideration should be given to converted qualitative data for use in driving decisions for infrastructure development in the near future, while focusing mostly on architecting the real metrics that will be useful in the out years to drive the smart technologies that will provide the energy and, hence, mission, assurance needed to support DoD operations.

# 6. Compilation of Current Literature

**Table 1– Negative Installation Impacts Literature**

| Title/ Author(s)/ Organization | Published |
|---|---|
| **Application of a Resilience Framework to Military Installations: A Methodology for Energy Resilience Business Case Decisions**<br>*Author(s): Judson, Nicholoas, Pina, Alexander L, Dydek, E. V., Van Broekhoven, Scott B., Castillo, A. S.*<br>*Org(s): MIT Lincoln Laboratory Lexington United States* | 2016-10 |
| **Uninterruptible Power Systems: Operational and Cost Considerations**<br>*Author(s): Milakovich, Marko, Jacobs, Charles E.*<br>***Org(s):** Air Force Communications Service, Scott AFB, IL Operations Research Analysis* | 1977-03 |
| **Valuing Air Force Electric Power Resilience: A Framework for Mission-Level Investment Prioritization**<br>*Author(s): Kwartin, Robert, Alexander, Sarah, Anderson, Martin, Clark, Donald, Collins, John, Lamson, Chris, Martin, Garrett, Mayfield, Ryan, McAlpine, Lindsay, Moreno, Daniel*<br>***Org(s):** RAND Corporation Santa Monica, United States* | 2019-01 |
| **Microgrid Study: Energy Security for DoD Installations**<br>**Author(s):** *Chen, Charles, Brown, Austin, Cheung, Kerry, Balwin, Sam, Creesko, Joe, Bindewald, Gilbert, Edmonds, Jae, Crozart, Matt, Daniels, Jarad, Clark, Corrie*<br>***Org:** Massachusetts Institute of Technology (MIT)* | 2012-06 |
| **Air Force Installation Energy Assurance: An Assessment Framework.**<br>**Author(s):** *Anu Narayanan, Debra Knopman, James D. Powers, Bryan Boling, Benjamin M. Miller, Patrick Mills, Kristin Van Abel, Katherine Anania, Blake Cignarella, Connor P. Jackson*<br>**Org:** *RAND Corportation (Project AIR FORCE)* | 2017-01 |
| **Smart Power Infrastructure Demonstration for Energy Reliability and Security (SPIDERS) Final Report**<br>**Author(s):** *Anderson,William W.*<br>***Org:** NAVAL FACILITIES ENGINEERING COMMAND PEARL HARBOR HI PEARL HARBOR United States* | 2015-12 |
| **Projecting Future Costs to U.S. Electric Utility Customers from Power Interruptions**<br>**Author(s):** *Peter H. Larsen, Brent Boehlert, Joseph H. Eto, Kristina Hamachi-LaCommare, Jeremy, Martinich, Lisa Rennels*<br>***Org:** Energy Analysis and Environmental Impacts Division Lawrence Berkeley National Laboratory* | 2017-01 |

# 7. References


[1] B. Strogen. "Attributing (negative) Value to Electricity System Outages at Military Installations." 8 June 2020.

[2] U.S. Evaluation of an Energy Resilience Analysis Tool for Army Installations. OSD Energy Resilience Assessment v5.1, July 2019

[3] RAND: Project Air Force. "Air Force Installation Energy Assurance: An Assessment Framework." 2017

[4] Hubbard, Douglas & Seiersen, Richard. "How to Measure Anything in Cybersecurity Risk." Wiley 2016

[5] National Institute of Standards and Technology (NIST). "Framework for Improving Critical Infrastructure Cybersecurity." April 16, 2018.

[6] Department of Homeland Security. "DoDCAR/.Govcar." Retrived from: https://csrc.nist.gov/CSRC/media/Projects/cyber-supply-chain-risk-management/documents/SSCA/Fall_2018/WedPM2.2-STARCAR%20SCRM%20FINAL%20508.pdf.

[7] Castillo, Ariel. " Department of Defense Installation Energy Resilience," June 8 2017.