InfraGard Critical Infrastructure Resilience Using System Engineering Techniques

By Casey Shull, PhDc, Eric Dietz, PhD, and Bob Kenley, PhD

Is North America vulnerable to wide spread electrical blackout from natural or man-made disasters? The short answer is yes. However, there are two distinct electrical systems operated by electric utilities. One, the bulk electric transmission system (BETS) transmitting high voltage electricity between states as a commodity between electric utility owners. Two, the electrical distribution system which delivers electricity at lower voltages to consumers including electrical service to critical infrastructure is generally confined to electric utility territorial boundaries. Plans for electrical restoration have been developed and are continually refined and simulated to ensure restoration of electricity after electrical outage within the BETS. However, electric utilities are not required by federal or state regulators to develop models to restore the electrical distribution system which serves critical infrastructure. Electrical distribution is restored according to reliability indices to minimize the duration of outage to customers by restoring the largest number of customers minimizing total outage duration. Thus, total number of customers are prioritized for restoration without consideration to restoration of critical infrastructure.

Current[1] and historical [234] literature identifies the electrical distribution systems as vulnerable to wide spread electrical outage creating security risks and wide spread socioeconomic chaos. Model based system engineering tools and techniques provides the systematic logic to provide a model for incremental electrical distribution restoration, applicable to every electrical distribution system, which will provide produce incremental electrical service to critical infrastructure thereby mitigating security risks and socioeconomic chaos.

Introduction

The Transmission System

Electricity has become a necessity to provide power for the infrastructure that has been developed to sustain the systems that support the growing human population in North America. Transportation, communication, health care, food, clean water, waste removal, security and other systems utilize electricity for daily operations to provide services to the population. "Thus, modern societies have become totally dependent on an abundant electricity supply."[5] "The structure of electricity delivery can be categorized into three functions: generation, transmission, and distribution, all

[1] National Academies of Sciences, Engineering, and Medicine. (2017). *Enhancing the Resilience of the Nation's Electricity System*. Retrieved from https://www.nap.edu.
[2] North American Electric Reliability Corporation. (December 9, 2017). http://www.nerc.com.
[3] PPD-21 Critical Infrastructure Security and Resilience (February 12, 2013).
[4] PPD-8 National Preparedness (March 30, 2011).
[5] Rudnick, H., Rivier, M. A., & Perez-Arriaga, I. J. (2008). *Electric Energy Systems-An Overview*. (Ch. 1). Retrieved from https://doi.org/.

of which are linked through key assets known as substations."[6 7]

Figure 1: Diagram of Electricity Delivery

The electrical system consisting of steel towers and/or wood poles and wires in North America are divided into two distinct systems; the high voltage Bulk Electric Transmission System (BETS), and lower voltage distribution systems. Transmission and distribution voltages are divided by the capacity or voltage class as shown in Table 1 below.[8]

The purpose of the BETS is to transport electricity at high voltages between power plants and/or electric utilities in different locations or states to be transformed into a lower voltage distributed to various types of consumers of electricity. The BETS is electrically interconnected among states transmitting high voltage electricity between utilities via physically interconnected conductors and sold as a commodity resulting in financial transactions between electric utilities. The technical transmission and financial transactions between utilities are managed and regulated by various federal and state government agencies. The federal agencies, Federal Energy Regulatory Commission (FERC) and North American Electric Reliability Corporation (NERC) and multistate Regional Transmission Operators (RTO), develop rules that compel electric utilities to develop and simulate plans for recovery if portions of the transmission system experience outage or blackout.[9] The transmission interconnection is divided into regions and managed by federal and state organizations as shown in Figure 2 below.[10]

Table 1: Description of Transmission and Distribution Voltage Classes

Description of transmission and distribution voltage classes

Power Line Classification	Voltage Range (kV)	Purpose
Ultra High Voltage (UHV)	>765kV BETS	High Voltage Transmission > 765kV
Extra High Voltage (EHV)	345, 500, 765	High Voltage Transmission or BETS
High Voltage (HV)	115,138,161,230	
Medium Voltage (MV)	34, 46, 69	Sub-transmission
Low Voltage (LV)	< 34	Distribution for residential or small commercial customers, and utilities

Note. Source: U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability

[6] Office of Electricity Delivery and Energy Reliability. (2015). *United States Electricity Industry Primer* (DOE/OE-0017). Retrieved from https://www.energy.gov.

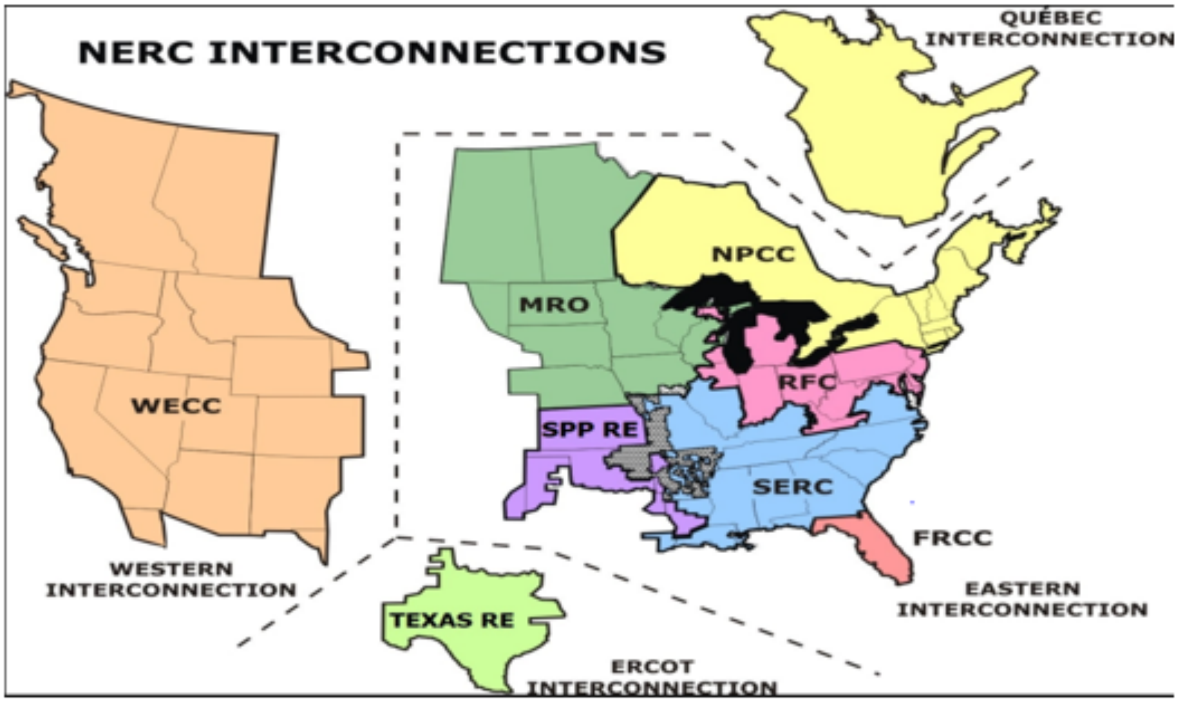
[7] www.energy.gov.

[8] U.S. Department of Energy, Office of Electricity Delivery and Energy Reliability.

[9] North American Electric Reliability Corporation. (December 9, 2017). http://www.nerc.com.

[10] www.nerc.com.

Figure 2: NERC Map Showing Interconnection between Regions



The BETS has inputs from multiple generation sources and is interconnected nationally through thousands of miles of high voltage transmission conductors providing the ability to transmit electricity to multiple regions. The high voltage transmission is transformed into lower voltage, referred to as electrical distribution, which is the location where the majority of electrical outages occur and the location to apply a model for incremental recovery. "Data indicates that 90% of

Figure 3: Diagram of Power Production Sources Feeding the Interconnected BETS and Substations to Transform Electricity for Distribution to Customers

customer outage-minutes are due to events that affect local distribution systems."[11]

Figure 3 above, although elementary in appearance, provides a diagram of the electrical system divided between power production, high voltage transmission and the lower voltage distribution in the U.S. [12]

The source to provide electrical transmission can be derived from fossil fuels, nuclear or renewables. However, the existing system of transporting electricity is the utilization of transmission and distribution facilities. The transmission system is regulated and managed by various organizations using resilience metrics, or the ability to resist, while the distribution system is not required to have resilience metrics. The purpose for the rules and regulations imposed by federal and state organizations are to make the BETS resilient to electrical outage and/or provide methods to recover from electrical transmission outage. Resilience is the "ability to resist, absorb, recover from or successfully adapt to adversity."[13] Resilience is commonly used as a requirement imposed by federal and state organizations compelling electrical transmission owners to develop and simulate plans for electrical transmission recovery. The goal of mitigating or eliminating electrical outage in the BETS is to prevent negative affects to consumers and financial markets as a result of electrical outage.

The Distribution System

Electric utilities whom are the owners and managers of the lower voltage electrical distribution system, 34kV and below, in the U.S. are vulnerable to damage causing widespread electrical outage. The distribution system is not managed or regulated by FERC, NERC or RTO's but reliability metrics, not resilience, are imposed by state and local regulators. "Reliability is the ability of the system or its components to withstand instability, uncontrolled events, cascading failures, or unanticipated loss of system components."[14] Therefore, reliability describes the stability of electrical distribution or the duration required by the electric utility to restore distribution electricity to consumers after an event causes blackout. The individual distribution systems are managed by individual electric utilities and the reliability of the system is monitored by state regulators through various reliability indices developed and defined by the Institute of Electronic and Electrical Engineers (IEEE) standard IEEE 1366-2012.[15] "Metrics for generation and transmission are used by FERC and NERC, whereas oversight of reliability at the distribution level is left to state regulatory agencies."[16] Health and welfare of the public, resilience, safety and security are dependent upon electrical distribution owners whose metrics are derived from the duration of

[11] Folga, S. M., McLarmore, M. R., Talaber, L. E., & Tompkins, A. M. (2016). *National Electricity Emergency Response Capabilities*. Retrieved from https://www.energy.gov.

[12] www.netl.doe.gov.

[13] Homeland Security. (2008). *DHS Risk Lexicon* p. 23 [Lexicon]. Retrieved from https://www.dhs.gov.

[14] U.S. Department of Energy. (2017). *Glossary of Terms*. Retrieved from https://www.energy.gov.

[15] IEEE Std. 1366-2012. *IEEE Guide for Electric Power Distribution Reliability Indices*. New York: IEEE, 2012.

[16] National Academies of Sciences, Engineering, and Medicine. (2017). *Enhancing the Resilience of the Nation's Electricity System*. (p. 31) Retrieved from https://www.nap.edu.

electrical outage experienced by the total number of electrical consumers affected. Indeed, maximizing efforts to restore electricity minimizing the outage to a large group of consumers provides a metric to measure an electric utilities efficiency in restoration efforts. However, restoration of power to critical infrastructure facilities is not enforced and/or there are no standards that establish rules or compelling reasons for an electric utility to develop a plan or model to restore electricity to critical infrastructure. The current methods of electrical distribution restoration do not have and/or require models for recovery and do not begin until the disaster has ceased and the assessment of repair, models and plans for recovery can begin. Electric utilities rely upon a network of "mutual assistance from other electric utility resources to respond to large natural disaster to restore damaged facilities and areas devastated by a disaster."[17] The restoration process requires days, weeks and in some cases months of reconstructing wood poles, installation of electrical wires and facilities before normal consumer activities can resume. Thus, the IEEE 1366 reliability indices allows the electric utility to self-report the total minutes of customer outage, or duration of outage within the distribution system, providing the utility with an incentive to restore the largest number of customers as efficiently as possible. Indeed, the current method of restoring damaged and devastated electrical facilities must continue in response to natural or manmade disasters. However, disasters causing widespread electrical outage are generally concentrated to a region where all available resources are being utilized within a utilities territory. Therefore, mutual assistance might arrive days after the event has ended due to availability of mutual assistance technicians increasing the time required to provide restoration of power to CI for health, safety and security. Thus, the development of a model to provide procedures and processes for incremental restoration to CI after a disaster caused electrical outage will mitigate, assist and/or prevent morbidity and mortality rates, resulting from the loss of electricity.

> Lecomte (1998) estimated that the 1998 ice storm that disrupted power to 1,673,000 customers, of whom 1,393,000 were in Quebec, resulted in economic losses of $1.6 billion in Canada and $1 billion in repair costs to the Hydro-Quebec and Ontario Hydro systems. A significant fraction of the 28 deaths in Canada and 17 deaths in the United States also resulted from the lack of power.[18]

The common recovery system described in this paper could have mitigated the loss of life described in the aforementioned event in 1998. In addition, compelling electric utilities to adopt and implement a common recovery system to provide incremental electrical restoration prior to future wide spread manmade or natural disasters will assist in

[17] Folga, S. M., McLarmore, M. R., Talaber, L. E., & Tompkins, A. M. (2016). *National Electricity Emergency Response Capabilities*. Retrieved from https://www.energy.gov (p. 21).

[18] Lecomte, E. L., Pang, A. W., & Russell, J. W. (1998). *Ice Storm '98* [Research Report]. Retrieved from Institute for Catastrophic Loss Reduction website: www.iclr.org.

the mitigation of negative health, safety and security events.

The NAP (2017) published a Consensus Study Report by the Committee on Enhancing the Resilience of the Nation's Electric Power Transmission and Distribution System to identify weaknesses and vulnerabilities in both power systems and in part summarized the following recommendations directed to the Department of Homeland Security and the Department of Energy:

Recommendation 7 to DHS and DOE: DHS and DOE should work collaboratively to improve preparation for, emergency response to, and recovery from large-area, long-duration blackouts by doing the following:

• Working with state and local authorities and electricity system operators to undertake an "all hazards" assessment of the natural hazards faced by power systems on a periodic basis (e.g., every 5 years). Local utilities should customize those assessments to their local conditions. (Recommendation 3.2)

• Developing and overseeing a process to help regional and local planners envision potential system-wide effects of long-duration loss of grid power. (Recommendation 5.3)

• Evaluating and recommending the best approach for getting critical facility managers to pre-register information about emergency power needs and available resources. (Recommendation 5.5) Renewing efforts to work with utilities and national, state, and local law enforcement to develop formal arrangements (such as designating selected utility personnel as "first responders") that credential selected utility personnel to allow prompt utility access to damaged facilities across jurisdictional boundaries. (Recommendation 6.1)

• Building off existing efforts to manufacture and stockpile flexible, high-voltage replacement transformers, in collaboration with electricity system operators and asset owners and with support from the U.S. Congress. (Recommendation 6.6)

• Developing a model for large-scale cyber restoration of electricity infrastructure.[19]

Thus, the responsibility for organizing the operators of CI, developing plans and procedures, creating and implementing simulation and training exercises is the responsibility of the DHS and DOE. Homeland Security PPD-5,[20] PPD-8, and PPD-21 establish the framework to develop local methods and procedures for recovery in addition to the structure for the Department of Homeland Security and to provide appropriations to local and state departments for development, training and execution of methods and procedures for electrical recovery. Appropriations have not been made available to local and state agencies to develop plans and procedures to provide a model for electrical restoration. This paper provides a model for electrical restoration to provide incremental power to

[19] National Academies of Sciences, Engineering, and Medicine. (2017). *Enhancing the Resilience of the Nation's Electricity System*. Retrieved from https://www.nap.edu (p. 139).

[20] Homeland Security Presidential Directive - 5, National Incident Management System (NIMS) DHSPD § 5 (2003).

CI after a wide spread manmade or natural disaster has caused a wide spread blackout.

Methods & Procedures

The methods to identify priority CI resides within the Department of Homeland Security (DHS). However, appropriations for DHS to begin methods and procedures for the development of a model for electrical distribution restoration will have to be developed into budgetary activities to fund the operations. Funding state and local budgets will allow the development of CI groups within local and state organizations to be managed by the local Homeland Security office to ensure consistent and continued training and application of procedures necessary for CI recovery. Identification of CI will need to be developed into prioritized locations to identify CI locations relative to electrical substations where the application of incremental electrical restoration will begin. The application of incremental electrical restoration will require the coordination of electric utility technicians and the operators and technicians of the CI locations identified as priority locations. Generalization of the method to provide incremental restoration can be described as isolating the transmission system feeding the local distribution system and consequently isolating the distribution system in the affected area. After isolation is complete, methods to provide incremental restoration to prioritized locations can be provided with a method of electrical generation that can attach to an electrical substation providing electrical service to a prioritized circuit feeding specific CI. Indeed, the method for recovery can be identified, however, the appropriations for the development of organized systematic restoration to pre-determined prioritized locations must be received to provide funding to develop the necessary activities for state and local emergency responders.

Procedures for Priority Locations

DHS has been identified as the primary organizing government organization to develop the local group of emergency responders. Priority locations to implement incremental electrical restoration to specific locations can be identified using Google Analytics in combination with applications from ESRI ARcGis software. Local electric utilities and emergency responders may have existing software to identify priority CI and aggregate the CI to the nearest electrical substation in conjunction with Google maps to provide specific GIS locations. The priority substation locations will be used as inputs into model based system engineering to customize the common recovery system for the electric utility adopting the modeling technique to provide incremental electrical restoration to CI.

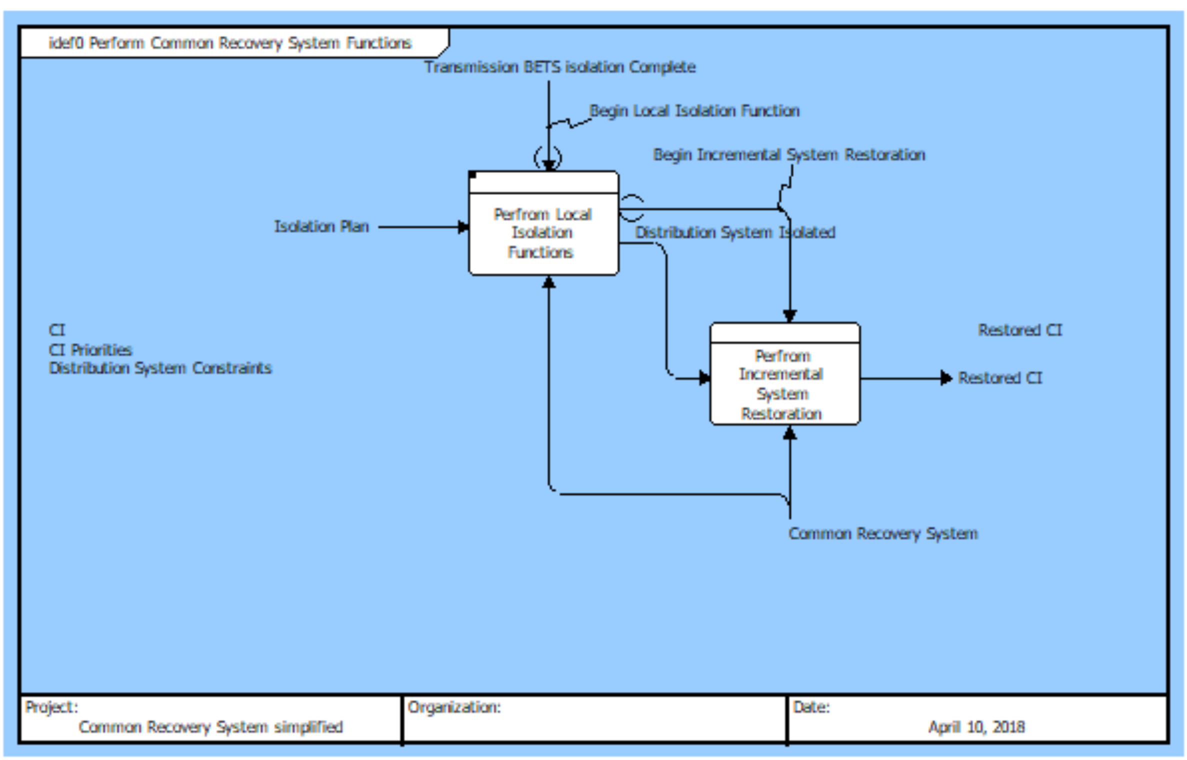
Model Based System Engineering

Model Based System Engineering (MBSE) or systems "is a construct or collection of different elements that together produce results not obtainable by the elements alone. The elements, or parts, can include people, hardware, software, facilities, policies, and documents; that is, all things required to produce systems-level results. The results include system level qualities, properties, characteristics, functions, behavior and performance."[21] Describing a system using graphical representations of how elements interact to produce a desired result among all collective stakeholders provides the simplification of processes necessary to provide incremental restoration. The basic model or process is to isolate the total electrical system affected and begin incremental restoration. MBSE provides the descriptive language using software products to simplify the complete process allowing the integration of complex software products into specific functions within the model allowing all CI operators to monitor and control CI through the complete recovery process.

The basic model, see Figure 4 below, describes the basic procedure using a high level diagram, Integration Definition for Function Modeling (IDEF0), identifying the primary components in the isolation to recovery process.

The system model is decomposed into additional elements showing inputs, arrows entering left side of function, that are transformed into outputs, arrows leaving the left side of the box, from the functional process inside the box. Processes and procedures are identified in graphical representations using MBSE to decompose or simplify each element and required task for the isolation and eventual incremental

Figure 4: Simplified IDEF0 model of Common Recovery System



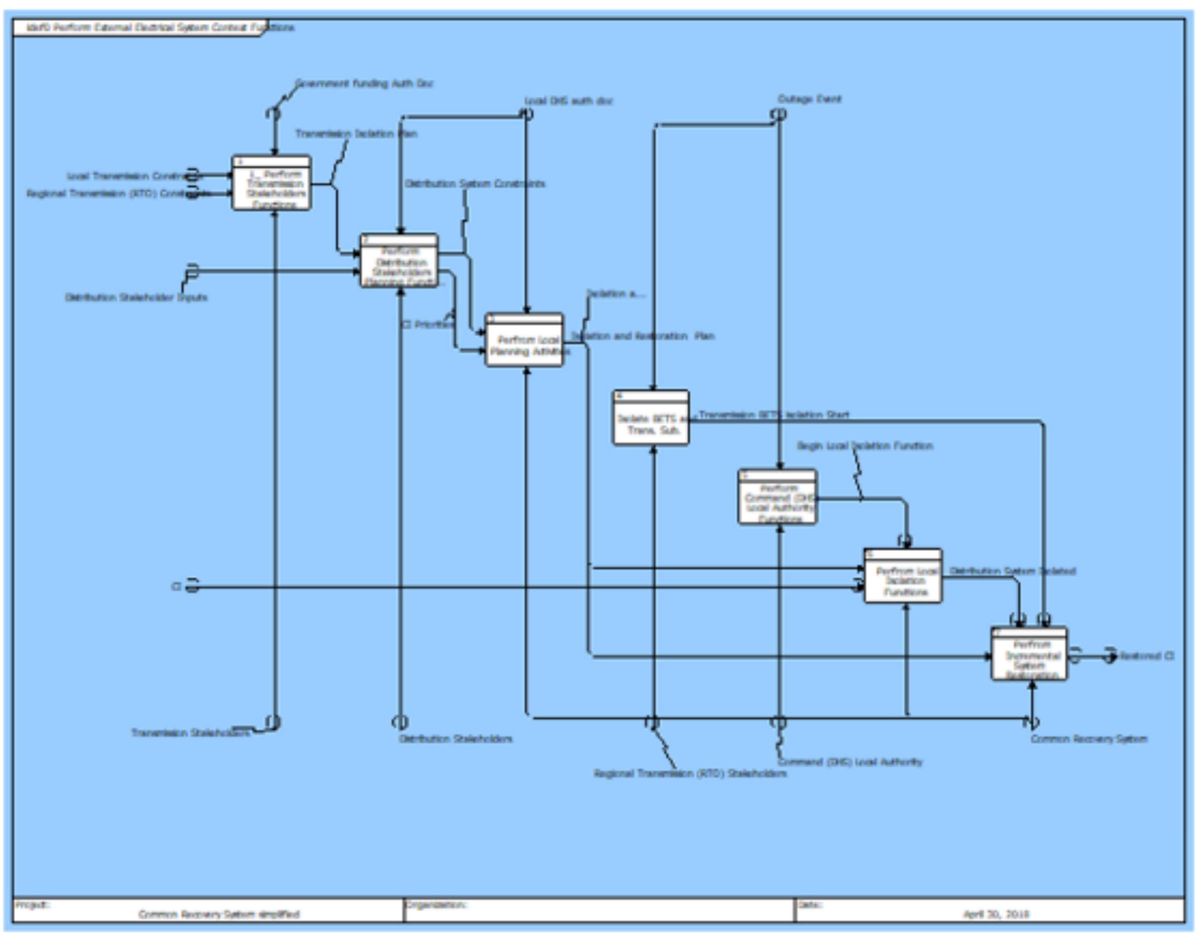
[21] International Council on Systems Engineering. Retrieved: https://www.incose.org/AboutSE/WhatIsSE (2017).

restoration of electrical distribution to provide power to CI necessary to provide safety and security.

Figure 5 below identifies the complete IDEF0 diagram from Government funding, system isolation to incremental restoration.

Each box depicted in the above figure can be decomposed into each simple element and or allow the integration of other software products for system operators to monitor and or manage the operation of individual CI. MBSE provides a high-level view that the incremental electrical restoration can be obtained providing all individual CI system operators provide necessary requirements for proper functionality of the model. The Common Recovery System depicted above can be adapted, with minor modification, to any electrical distribution system providing power to CI. Figure 6 below provides additional graphical representation of the system model.

Figure 5: IDEF0 Providing Graphical Representation of the Elements Required to Begin Incremental Electrical Restoration

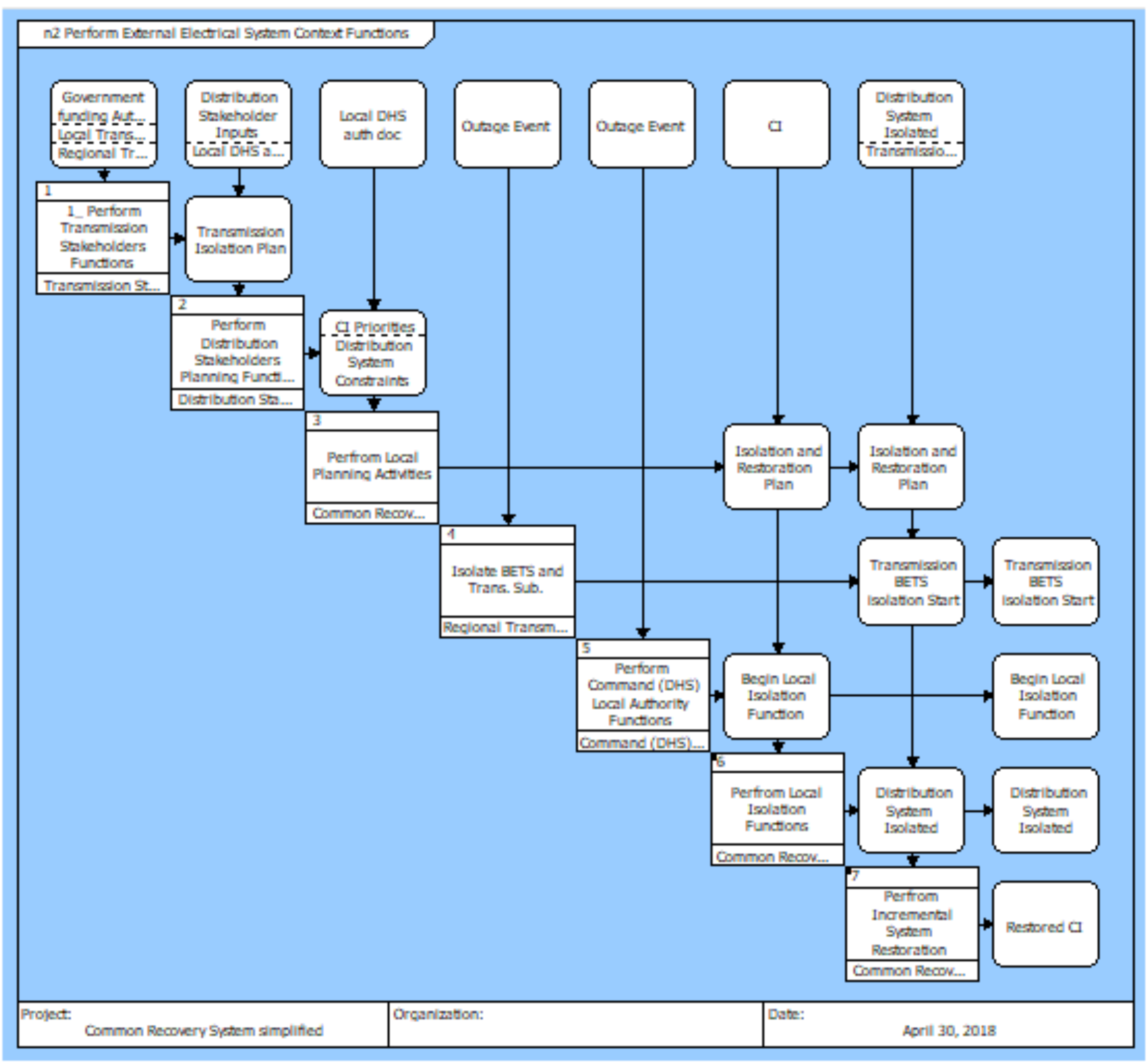


The functional behavior graphical representation above, known as an N2 diagram, identifies the functional components required to achieve the desired result, incremental electrical restoration of CI. The first or primary trigger to achieving incremental restoration to CI is funding or appropriations from the federal DHS to the local DHS to begin the process of aggregating all of the necessary CI into priority locations to provide inputs to MBSE providing a process of restoration.

Conclusion

Presidential Policy Directives, National Academies Press, Congressional Reports and comprehensive studies produced by technical organizations identify the need for action by the DHS and DOE to protect and defend the electrical distribution system in the U.S. However, no action has been taken

Figure 6: Functional Behavior Model of the Common Recovery System Providing Graphical Representation of Elements Transformed by Functions to Achieve Electrical Restoration



due to the requirement of appropriations from the federal budget to be distributed to the state and local organizations tasked with maintaining the safety and security of the U.S. population. The federal government has provided plans, processes, requirements and compelled electric utilities to simulate, validate and verify the plans and procedures for the BETS on a bi-yearly basis. But, the distribution system which serves the CI at the local level has been entrusted to its operation by local organizations and electric utility owners. Thus, the electric distribution system is vulnerable to attack causing wide spread electrical blackout which will create socioeconomic chaos. Appropriations must be developed at the federal level to provide local DHS responders the funds to prepare, train and validate plans and procedures for incremental electrical restoration after a wide spread natural or terrorist EMP attack. The common recovery system developed using MBSE provides a systematic and universal method to provide plans and procedures for incremental electric recovery to CI mitigating socioeconomic chaos.