Implementation of a Holistic Risk Framework for Critical Infrastructure

Merideth Secor[a], Derek Koolman, II[a], Robert Greer[a], Jason Reinhardt[b], Samrat Chatterjee[c], Kathleen Hill[d], Eric Watkins[d]

[a]Cybersecurity and Infrastructure Security Agency (CISA), Arlington, Virginia
[b]Sandia National Laboratories, Albuquerque, New Mexico
[c]Pacific Northwest National Laboratory, Richland, Washington
[d]Systems Planning and Analysis Inc, Alexandria, Virginia

Abstract: The Cybersecurity and Infrastructure Security Agency (CISA) leads the national effort to understand, manage, and reduce risk to our cyber and physical infrastructure, and must assess risks that cover a broad range of threat scenarios over a complex set of interdependent critical infrastructure systems. Within CISA, the National Risk Management Center (NRMC) is responsible for providing analysis and insight on all risks, across all critical infrastructure at the national scale. Since 2019, CISA's NRMC, through the National Infrastructure Simulation and Analysis Center (NISAC), has been developing and implementing a framework based on the 55 National Critical Functions (NCFs) to provide a functional view of the United States critical infrastructure. While an asset-focused view of critical infrastructure describes how assets are integrated geospatially, and an entity-focused view describes how infrastructure is managed and owned, the functional view describes the services that the infrastructure enables for the nation to ensure a standard for security and way of life. To create this functional framework, the NCFs have been decomposed into a network of subfunctions that are connected via dependencies within and across the NCFs. The functional network provides an overarching foundation to conduct analysis on risk-informed decisions across the entire risk landscape, revealing connections between different critical infrastructure sectors, such as cross-sector emerging risks and functional dependencies. The resulting network graph produced from these decompositions comprise the functional lens of the underlying analytic framework leveraged by the Suite of Tools for the Analysis of Risk (STAR), formerly known as the Risk Architecture. Previous research has laid out the concepts and principles behind the initial framework; this paper presents the implemented analytic framework, demonstrates an example application of the produced network graph data, and discusses the lessons learned while working to refine the NCF Decompositions.

Keywords: Infrastructure, Ontology, Methodology, Network Graph

1. INTRODUCTION

In today's interconnected society, the United States faces a wide array of serious risks from many threats, all with the potential for significant consequences that can impact our National Critical Functions (NCFs). These functions are built as "systems of systems" with complex designs, numerous interdependencies, and inherent risks. While this structure allows for significant gains in efficiency and productivity, it also exposes the United States to risks that undermine our national security, economic prosperity, and public health and safety. The Cybersecurity and Infrastructure Security Agency (CISA), within the United States Department of Homeland Security (DHS), is charged with leading the national effort to understand, manage, and reduce risk to the cyber and physical infrastructure Americans rely on every hour of every day. Within CISA, the National Risk Management Center (NRMC) works with government and industry partners to identify, analyze, prioritize, and manage the most significant and systemic strategic risks to the nation's critical infrastructure. The NRMC specializes in building data, methodologies, models, and tools to analyze risk to critical infrastructure from multiple angles and provide actionable products and insights to decision makers so they can reduce their risk and enhance their resiliency.

1.1 Background

In April 2019, CISA published its initial set of 55 NCFs [1], which have since been complemented by definitions for each function. The effort to identify and define these critical functions was conducted in collaboration with government and industry partners associated with all 16 CISA critical infrastructure sectors [2], state, local, tribal, and territorial (SLTT) government partners, and other stakeholders. NCFs are functions

of government and the private sector so vital to the United States that their disruption, corruption, or dysfunction would have a debilitating effect on security, national economic security, national public health or safety. The NCFs represent an evolution to the critical infrastructure risk management framework established in the National Infrastructure Protection Plan [3] and are applied across CISA [4]. While the previous approaches focused almost entirely on owners' and operators' risk management as opposed to outcomes to the nation due to cascading risks, the NCF approach enables a richer understanding of how entities come together to provide critical functions and what assets, systems, and technologies underpin those functions.

By viewing risk through this functional lens, NRMC provides a cross-cutting, multidimensional view of risk to critical processes, infrastructure, and assets, which NRMC can use to better understand national-level and systemic risk that could cause broad, cascading impacts across sectors. This allows for the ability to add resilience and harden systems across the critical infrastructure ecosystem in a more targeted, prioritized, and strategic manner. The value of NCFs is in both their ability to convey the complexities and dependencies of critical infrastructure, and their effectiveness as a framework through which to develop data and advise critical infrastructure stakeholders. To effectively analyze risks to the critical infrastructure, CISA must be able to easily access diverse data sources, including the NCFs, and incorporate these datasets together with model-based capabilities into a standardized, reproducible analytic framework.

In 2022, CISA presented its approach to understanding, managing, and reducing risk to the nation's cyber and physical infrastructure via the development of the NCF Framework, developed from decompositions of the NCFs, to incorporate information on the operation and interdependencies of critical infrastructure [5]. This work described both the functional lens through which critical infrastructure analysis can be approached, as well as the basic graph structures used to represent and analyze interdependencies and facilitate a foundational common understanding of the NCF structure. At this time, CISA introduced the Risk Architecture as a way of incorporating this information, integrating layers of analytic capabilities consisting of assessment frameworks and tools, analytic models and data, and additional critical infrastructure datasets. This proof-of-concept Risk Architecture tool has been subsequently developed to include additional data and analytic capabilities and has been expanded into the Suite of Tools for the Analysis of Risk (STAR).

Many authors have examined critical infrastructures as networks of interconnected assets [6], interconnected networks of assets [7], or as asset networks with time-varying properties and incomplete information [8]. Lindstrom and Johansson proposed modeling critical flows between nodes arranged on a graph as one method for identifying important nodes [9] [10] [11]. Others have looked at fundamental robustness [12] or resilience metrics [13] as feature of network structures. Functional decompositions have been applied to create models of corporate information systems to aid in incremental modernization efforts [14]. What follows extends previous work presented in this forum [5], and advances the state-of-the-art of critical infrastructure risk assessment literature by developing and applying a functional decomposition approach to augment asset-based networks with the aim of improving scalability of analysis.

1.2 Holistic Approach to Critical Infrastructure Risk Analysis

The previously described functional perspective actioned through the NCF Framework serves as one of three analytic lenses used for critical infrastructure risk analysis that aims to fully examine the critical infrastructure risk landscape, alongside asset and entity perspectives. The functional perspective aims to classify the processes and services provided by the nation's critical infrastructure assets and characterize how these functions are interrelated. The asset perspective aims to determine what are the critical infrastructure facilities of interest, where are they located, and what dependencies exist amongst them through which resources or services are provided. The entity perspective aims to align the physical infrastructure facilities to owners, operators, and regulatory agencies to identify the stakeholders responsible for management, mitigation, and prevention of critical infrastructure risk. The latter two perspectives are enabled by the All-Hazards Analysis (AHA) dataset developed by Idaho National Laboratory that captures the physical location of over two million infrastructure facilities, along with unique attributes such as their owners and operators. At the center of these three perspectives, or lenses, sits CISA's critical infrastructure sectors, those sectors whose, "…assets, systems, and networks, whether physical or virtual, are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on security, national economic security, national

public health or safety, or any combination thereof" [2]. The taxonomical breakdown of the sectors through the Infrastructure Data Taxonomy (IDT) provides a framework which serves as a basis to bring these lenses into alignment and incorporate sector-specific stakeholder expertise. CISA's risk strategy is to action these analytic lenses through the development and/or procurement of relevant datasets, incorporating them into a singular, holistic risk framework that will be leveraged within STAR to facilitate infrastructure analysis.

2. NATIONAL CRITICAL FUNCTION DECOMPOSITIONS

2.1 Functional Decompositions

As described previously, CISA decomposed the NCFs to use the functional perspective of the critical infrastructure risk framework. To fully realize the analytic potential of this perspective, CISA is working to enhance the understanding of the subfunctions and interdependencies that comprise each NCF and how they connect to infrastructure systems, assets, and components. A functional decomposition generally refers to the process of breaking down the functions of large, complex systems into their constituent units of analysis. When applied to critical infrastructure, this process breaks down NCFs into subfunctions of various levels of granularity, which together represent the processes required for an NCF to operate.

At the most basic level, the result of the NCF Decompositions is a network graph database. A network graph database is made up of nodes, edges, and corresponding attributes to represent data that is based on structured relationships. The nodes of the graph represent the NCFs and subfunctions that increase in granularity as you move down the decomposition structure. The edges of the graph represent relationships between those nodes, capturing the dependencies between each NCF or subfunction. Edges can then be given properties that further describe the nature of the dependency, such as its degree (i.e., strength) or type. As the data in a graph database is optimized for relational queries, users can quickly explore these relationships and capabilities to use them to create effective models and simulations to facilitate risk analysis within STAR.

2.2 Initial NCF Decompositions

From creation of the NCFs in 2019 through mid-2022, CISA worked to mature this consequential dataset with very limited guidance or overarching structure. The initial decompositions were shaped by representatives from Community of Interest (COI) partners, who provided subject matter expertise on the definitions and subfunctions of an NCF. CISA also had multiple research teams conducting initial decomposition efforts resulting in a graph of over 3,500 functional nodes and their associated dependencies. Initial versions of decompositions from this team spanned a range of approaches, content, and depth. Some were functionally focused while some leaned more toward asset taxonomies, which resulted in difficulties during integration and analysis. Despite these difficulties, this process allowed for the discovery and development of best practices both for the analytic approaches used and the decomposition structure itself. It also highlighted the need to establish a unified analytic approach to the NCF Decomposition methodology and a set of common standards that could unify decomposition data and dependency analysis for future versions.

3. NCF DECOMPOSITION DATA MATURATION STANDARDS

Based on the lessons learned from the initial NCF Decompositions, data improvement requirements were identified for increased process consistency, maximized data buildout, and more granular dependency linkages. These improvements help improve data transparency, enhance analysis across the NCF Framework, and enable analysis that spans and combines the analytic lenses of the critical infrastructure risk framework described previously. To meet these goals, the NCF Decomposition data maturation process was developed with four main objectives to be carried out by their own associated step with the assistance of multiple National Laboratory performers and contract support teams. The full methodologies associated with each of these data maturation steps will be released publicly through CISA in late 2024 as a complement to this paper, and further details can be requested by contacting the corresponding author. The following section summarizes each of these steps, as framed by their associated analytic objectives below:

1. **Decomposition Structure:** Produce a standard decomposition structure across all support teams and across all 55 NCFs
2. **Decomposition Verbiage:** Standardize the content of subfunction names and definitions
3. **Decomposition Mapping to Asset Taxonomy:** Execute a data mapping from NCFs to CISA's IDT

4. **Decomposition Dependencies:** Identify critical dependencies within and across all NCFs

3.1 Decomposition Structure

To produce a standard decomposition structure across all support teams and across all 55 NCFs, the methodology applied minimizes dissimilar or contrasting interpretations between the various parties carrying out the development of the decompositions. The team identified various ontologies for potential application to the NCF Decomposition functional use case, which spans a wide variety of systems. One such methodology examined was the Function-Behavior-Structure (FBS) approach, which for this application would discuss the relationship functions have with their expected behaviors, structures have with their emergent behaviors, and the interplay between the two types of behaviors. While methodologies explored were numerous and diverse, the FBS approach is well documented and aligns with the process required to develop an NCF into its decomposition [14]. This FBS methodology can be used to describe all designed things with the three fundamental constructs defined below:

- **Function (F):** the purpose of the object, or what the object is for
- **Behavior (B):** the attributes that can be derived from the structure, or what the object does
- **Structure (S):** the components of the object and their relationships, or what the object consists of

When applying FBS ontology to the decomposition of an NCF, we can expand the standard FBS levels described above to the four levels of the NCF structure. These levels are described as follows:

- **1st Functional Level (NCF):** The NCF Requirement
  - Example: Produce and Provide Agricultural Products and Services (PPAPS)
- **2nd Functional Level:** The functions that are required to achieve the NCF through a set of Actions
  - The infrastructural functions required, as well as "Management," and "Regulations, Standards, Licensing, and Agreements," all beginning with "Perform…"
  - Example: Perform Agricultural Production for PPAPS
- **3rd Functional Level:** The Expected Behavior (Be) based on the functions
  - NCF behaviors: Operate, Maintain, Support, Connect
  - Example: Operate Production for PPAPS
- **4th Functional Level:** The Structural Behaviors (Bs) that are derived from the structure
  - NCF Structural Behaviors: Operations each system carries out to help achieve the Be
  - Example: Distribute Water for Raw Product for PPAPS

The NCF Actions (2nd Functional Level) are abstract in nature and required significant effort to understand and develop. Before finalizing the Actions for each NCF, existing DHS, academic, and business documents and diagrams were reviewed to ensure sufficient aggregation of expertise. It was then determined that two additional actions were needed and must then be added if not already accounted for in the background research: "Perform Management for NCF" and "Perform Regulations, Standards, Licensing, and Agreements for NCF." The 3rd Functional level of FBS Decomposition is comprised of four Be that further describe each of the NCF Actions. Of these Be, the essence of each NCF is represented through the Operate Be and the three secondary Be (i.e., Support, Maintain and Connect) that enable performance of the Operate Be. The Bs, or Operations, that make up the 4th Functional Level of the NCF Decomposition are developed using a set of recommended verbs determined by which Be they fall under.

3.2 Decomposition Verbiage

To further ensure consistency of the decompositions between NCFs and their resulting application to critical infrastructure risk analysis, the team developed rigorous verbiage guidelines and checks for the subfunction titles and definitions, as part of the FBS Decomposition methodology. This standardization of verbiage is a crucial stage in the NCF Decomposition process and was enforced through a process called the Verbiage and Consistency Check (VAC). This process involved a series of checks to verify that the decomposition adheres to the correct functional and naming structure, as well as the appropriate verbiage guidelines, as described in the FBS Decomposition Structure documentation. The lexicon for subfunction verbs were restricted to a specific set of pre-defined words, each with corresponding definitions to ensure consistency and clarity in subfunction interpretation. The VAC process used Natural Language Processing (NLP) to assist in validating

whether a given decomposition aligned with the FBS rules concerning naming, verbiage, and functional structure.

3.3 Decomposition Mapping to Asset Taxonomy

CISA's previous contribution to PSAM 16 describes the expansion of the NCF Decomposition lens from the functional to physical (or asset) infrastructure perspective as described above, enabling the evaluation of the physical facilities which support the functionality of NCFs and their influence across the NCF Framework [5]. The NCF Decomposition dataset is linked to the physical or asset critical infrastructure captured in the AHA dataset through an intermediate classification system, the IDT. The IDT Version 4, which was issued by the DHS Office of Infrastructure Protection in 2011, classifies infrastructure assets through a taxonomy decomposing each sector to describe the varied types of facilities which make up the nation's critical infrastructure network, acting as a "Rosetta Stone" to link multiple datasets within STAR. Functional analysis focused on NCFs and their subfunctions can be expanded through these connections to the IDT's asset classes that enable the most granular functionalities; subsequently serving as a link to the actual critical infrastructure facilities which carry out each subfunction.

An Analytic Sufficiency Check (ASC) was conducted as a part of the data maturation process to validate that the decomposed NCFs have complete linkages to the IDT, ensuring that physical asset-level data can be connected to NCFs in support of risk analysis across NRMC and CISA. This process focused on accomplishing the following three objectives; (1) to ensure that all Operations at the 4th subfunction level are mapped to one (or more) IDT asset class, and that all IDT asset classes that carry out the process represented by the subfunction in question are included in the mapping regardless of their sector; (2) to ensure that all mappings occur at the lowest level possible of subfunction to the lowest level of the IDT taxonomical structure (e.g., all mapping occurring from a leaf of one taxonomy to the other); and (3) to ensure that only the IDT asset classes which directly carry out the function described in the subfunction are mapped. These objectives support risk analysis through the development of accurate and complete mappings across the functional nodes within the network. This mapping also enables an indirect link with other CISA data, analysis, and capabilities previously linked to the IDT.

3.4 Decomposition Dependencies

Within the NCF Framework, dependencies describe the relationships between the processes that combine individual subfunctions into decompositions and align the NCF set into a singular network. There are two types of dependencies that form the connections within each NCF Decomposition, referred to as Intra-NCF Dependencies; 1) the parent-child relationships that form the vertical links between the functional levels of the decomposition breakdown; and 2) the horizontal mappings between Operations at the 4th functional level (see Figure 1). These intra-dependencies are further characterized by edge attributes that apply logical conditions (i.e., dependency characteristics) or classify each dependency type (e.g., transactional, compositional, or procedural).

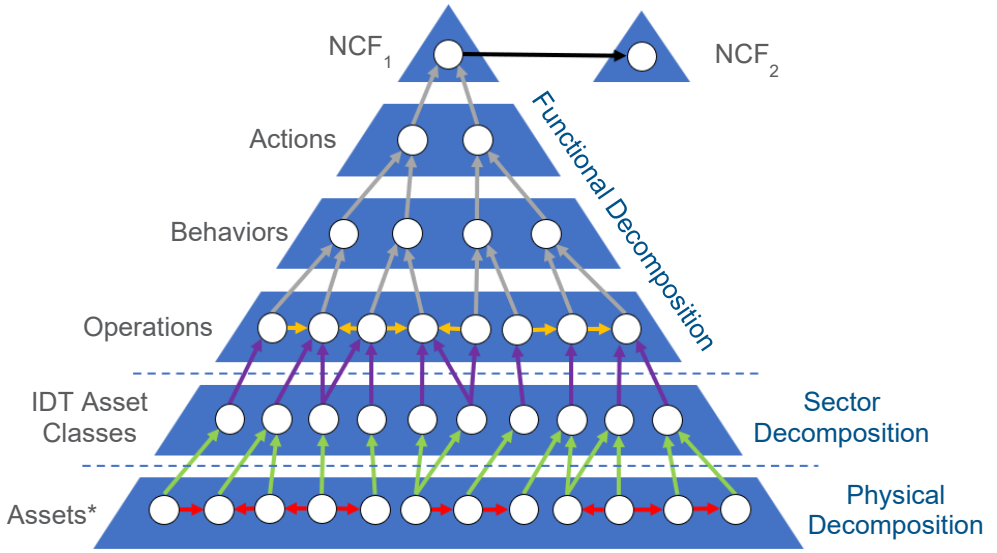
The NCF Framework also captures relationships between NCF nodes, referred to as Inter-NCF Dependencies. These Inter-NCF Dependencies were developed by first identifying a series of resources each NCF either provides for or requires for continued functionality (e.g., transportation, electricity, or communication) and then aligning the two mappings to create the NCF level edges within the network. These resources are then captured as an attribute on these edges to further describe the nature of the relationship within the network graph. While this method allowed for consistency in dependency identification, many second order or time delayed dependencies were inadvertently captured. To filter down this list of dependencies into alignment with the scope of analysis conducted at NRMC, only direct dependencies with a high impact and a time of effect of a week or less were included in the final dataset.

4. APPLICATION OF NCF DECOMPOSITIONS

4.1 Analytic Framework

The decomposition standards detailed in the previous section aim to produce functional decompositions that align with a holistic analytic framework connecting functions, assets, and entities, as described in Section 1.2.

Each NCF Decomposition can be notionally visualized as depicted in Figure 1, where network graph nodes are represented by the white circles with associated labels to the side of the pyramid and edges by the arrows of different colors.



Legend	Edge Description	Relationship	Key Attribute(s)		
	Inter-NCF Dependency	Provides For	Resource		
	Compositional Intra-NCF Dependency	Is Required For	Type	Characteristic	
	Non-Compositional Intra-NCF Dependency	Provides For	Type	Characteristic	
	Infrastructure Data Taxonomy Mapping	Performs	N/A		
	Asset Node Attribute	Is Classified As	N/A		
	Asset Dependency	Depends On	Type	Strength	Confidence
*	Assets include attributes for owner and operator data to connect Asset and Entity perspectives				

Figure 1: Notional Diagram of Analytic Framework with Associated Edge Information

Figure 1 describes the subgraph that each NCF and its decomposition represents; when consolidated, they make up the network graph that comprises the NCF Framework. As shown in the notional diagram, logical and physical dependencies are captured both vertically across the functional, sector, and physical decompositions, and horizontally within the functional and physical decompositions. Similar to the functional breakdown of the NCFs described above, the IDT can be viewed as a taxonomical sector decomposition originating at CISA Sectors. The fifth layer of the pyramid in Figure 1 depicts the asset class layer of one such decomposition, through which each NCF would not be limited to mappings to only one sector. The physical decomposition network breaks down real world systems into specific assets and their components (i.e., facility equipment). This physical lens will allow for the eventual connection of an entity subgraph that is planned to expand upon the information currently captured via owner and operator attributes of physical facility nodes. The edges of the NCF Framework detailed in previous sections are depicted as well, to include descriptions of each relationship and their key attributes. The combination of these vertical and horizontal connections across the analytic framework, allows for analysts to cross walk between these different network graphs to conduct a comprehensive assessment that attempts to answer a variety of risk questions for an individual scenario, as detailed in the following section, but also still be applicable to a wide variety of risk scenarios for critical infrastructure.

4.2 STAR Analytic Questions

The application of this critical infrastructure risk framework to risk analysis conducted by CISA analysts allows for both the identification of strategic impacts to national infrastructure functionality from point disruptions within the greater network, as well as the identification of an asset network that supports operation

of an NCF of interest. The initial proof-of-concept for STAR attempted to describe how an NCF operates by incorporating initial versions of the pyramid depicted in Figure 1, focusing on functional capabilities provided by system owners and the assets required to perform those operations. This top-down approach, however, limited understanding of potential cascading impacts across both NCFs and physical infrastructure. The continued evolution of STAR has focused on the development of data and capabilities to answer a series of analytic questions which begin by examining assets of a specific sector, continue to identify cascading impacts across the physical decomposition and asset-level dependency network, and ultimately contextualize the NCFs affected by an outage which originated at a specific asset in the network. The current implementation of STAR allows analysts to not only answer variations of those analytic questions presented in the previous submission across the entire NCF set [5], but also to answer the following set of expanded analytic questions which span from granular to strategic levels of analysis:

1. What water assets are contained within an area of concern?
2. What other critical infrastructure is connected to a water asset in our area of concern?
3. If that water asset is compromised, how are the connected critical infrastructure systems impacted?
4. What is the shortest failure pathway between two assets of interest?
5. Which asset is a priority based off of different network graph metrics?
6. Which NCF(s) are enabled by that prioritized asset(s)?
7. If that highly connected asset(s) was compromised, how would the failure propagate across NCFs?
8. What reports can be exported for the NCF directly associated with the highly connected asset?

These analytic questions frame analysis for a broad spectrum of potential use cases to inform decision making across the critical infrastructure risk landscape. Using a holistic risk framework allows U.S. government decision makers to examine critical infrastructure issues using any of the previously described analytic lenses –Physical, Sector, or Functional–as a starting point.

To answer these questions using STAR, analysts leverage the Physical lens as a starting point to populate assets that support the Water and Wastewater Systems Sector in an area of concern. Using the asset-level dependency network, analysts can further determine what other assets are dependent upon the water assets identified and highlight potential cross-sector risks to any of the other 16 U.S. Critical Infrastructure Sectors [2]. The Physical and Sector lenses, however, only provide a subset of the risks to the nation. For instance, a wastewater treatment plant may provide treated water through a series of pumping stations to a power generation facility that, in turn, generates electricity to be transmitted across a series of substations. The Physical lens or perspective helps the analyst evaluate only impacts along this path, providing an understanding of potential cascading impacts across the dependency network. This gives analysts a clear baseline understanding for analysis but does not adequately paint a holistic picture of risk to the nation. Traversing the network from the physical assets through the IDT provides a link to the Functional network, allowing analysts to highlight the Operations that the impacted assets support. Then analysts can use the functional decompositions as well as intra- and inter- dependencies to describe the potential for functional loss or degradation in a manner that is scalable across cities, states, regions, or a nation.

CISA developed STAR to integrate tools, data, methods, and models into a single web-based application. STAR leverages the foundational capabilities proven via the Risk Architecture prototype to provide an analytic engine for critical infrastructure risk analysis and expands upon the initial top-down analytic approach of NCFs to assets [5]. STAR also uses the network graph data structure described above to apply network statistics to critical infrastructure risk analysis. Network centrality measures are particularly helpful in identifying critical nodes among networks of like node types. Using the STAR application, analysts can visualize, describe, and analyze the entire NCF Framework depicted in Figure 1. Further, this allows U.S. government decision makers access to timely, repeatable, and actionable risk analysis focused on maintaining critical functions that provide for security, national economic security, and national public health or safety. STAR affords an all-hazards and all-threats approach to assessing risk to critical infrastructure and modeling potential mitigation strategies across a wide range of scenarios.

5. DISCUSSION

The development of a common methodology for functional decomposition of critical infrastructure systems

faced several challenges. It was critical to clarify semantics through development of lexicon and verbiage guidelines, prescribe levels of decomposition to be achieved, and develop functional dependency types and characteristics early in the process to enable the development of the NCF Framework across all 55 NCFs and all performers (See Section 3.1). When descriptively decomposing critical infrastructure systems through the functional decomposition process, it can be tempting to divide the system into kinds rather than more universal functions. For example, water supply might be divided into potable and non-potable systems, or drinking, irrigation, and grey-water systems. Certainly, each system has very different physical implementations due to differing requirements or geographical considerations. However, these are taxonomic rather than functional approaches, and tend to create many redundant nodes and edges in the network where disparate systems use function in a similar manner. Purely functional approaches are generally more robust than taxonomic decompositions. In addition to these issues, taxonomic methodologies also have the potential to create fragile structures as new system development over time can quickly invalidate the network. Further, these approaches tend to include information that would be better captured in asset-focused views of the system. That is, functional networks should capture what needs to be done to enable a NCF rather than how it's done. It is for these reasons that the FBS-based methodology was developed and implemented to create the NCF Framework.

Creating the first coherent functional decomposition of all 55 NCFs was a large undertaking that involved multiple teams across several institutions and multiple iterations. Based on the initial lessons learned, the approach detailed in this paper was validated across the set of analyst teams through a series of debates and the development of examples. Despite being geographically distributed, the individual teams collaborated via extended working sessions to share early findings, provide critiques, and harmonize results. Regular full team meetings ensured that results were achieved according to the developed methodology. At times, the teams needed to return to previously completed NCF Decompositions to adjust these drafts to incorporate findings identified in new decompositions. This high touch, iterative approach had the benefit of allowing multiple parallel teams to cover the broad scope of the NCFs while keeping the data generated consistent and integrated.

The functional network created by the decompositions of the NCFs creates a view of critical infrastructure that is agnostic to implementation and may also be agnostic to geographic scale or the nation that may use it. The same functional decomposition of NCFs can be applied analytically to a town, county, state, or region in the same way that it could be applied to a nation, and an NCF network developed for one nation theoretically could apply to another. The implementation of those functions as described in an asset-based view may be different, each nation developing its own IDT to describe unique features of its critical infrastructure sectors, but the same functional dependencies and potential cascading impacts would apply and allow analysts to understand risks. The decompositions generated so far are a significant step forward but will likely require further refinement as arguments about geographic and national fungibility are tested, and those refinements will make the results increasingly useful to a broader range of users. Collaborative efforts on functional approaches for critical infrastructure risks are necessary to continue working toward this vision.

6. NEXT STEPS

6.1 Exploration of Network Failure and Resilience

The NCF Framework in the form of a network graph provides an analytic construct through which one can explore regional and national level critical infrastructure risk and resilience against cascading failures [5], and may be used to develop node- and network-level risk and resilience metrics based on methods from graph theory, network science, and network optimization [15] [16] [17] [18] [19]. Components of risk as described in previous work [5] [20] (i.e., threat, vulnerability, and consequence) may be characterized based on likely orders of impact and network connectedness degradation along simulated failure cascade paths. Further, elements of NCF resilience including robustness, recovery, and adaptation [21] may be characterized via centrality-based dynamics to assess network functionality and optimal recovery pathways. Development of a flexible and modular computational codebase is currently in progress to develop and integrate models and simulations which use the data described above. Further advances toward an operational data-to-decisions compute workflow in STAR will require appropriate scaling of functional effects to and from real-world infrastructure context, and continued close collaboration between homeland security stakeholders, analysts, and scientists.

6.2 Additional NCF Decomposition Improvements

Additional refinements of the NCF Framework are achievable through various approaches to further improve the analytic utility of the dataset. While the FBS effort brought the NCF Decompositions into alignment to better allow for a comparison across disparate domains, this data might be matured to further clarify the scope of each subfunction. The mapping of subfunctions to the IDT asset classes similarly will need to be revisited upon the completion of Version 5 of the IDT, an ongoing project being carried out by CISA to ensure that it reflects the current realities of the critical infrastructure space, as well as to incorporate additional data validation efforts [22]. Future maturation of the network's dependency data consists of expanding the inter-NCF dependencies to map out linkages between Operations of different NCFs, as well as the build out and standardization of edge attributes across Inter- and Intra-NCF and Asset dependencies. Additionally, validation of these dependencies will be conducted using multiple approaches, including operational use-case testing as a comparison against real-world scenarios, as well as comparison against dependencies captured in other areas of the framework. NRMC will continue to improve and expand on the NCF associated datasets, working to incorporate additional taxonomies and critical infrastructure frameworks to enhance analysis according to CISA analytic requirements.

7. CONCLUSION

Developing estimates of risk across a wide range of hazards and scenarios on a disparate set of highly interconnected systems in the absence of complete and accurate data is a significant challenge. Decisions regarding risk mitigation measures, investments in resilience, responsive actions, and policies for governance of critical infrastructure must be made regardless of the current quality of those risk estimates or level of uncertainty about those systems. This paper describes application of a method for developing an improved, scalable approach to functionally describing critical infrastructure for risk analysis, thus adding an additional lens to traditional asset and owner approaches. The method described here can be leveraged and further refined by organizations and governments to improve critical infrastructure risk assessment capabilities and to enable increasingly systematic and rigorous assessments, as well as provide an improved framework for communication and collaboration.

Funding Disclosure

This research paper was supported by Sandia National Laboratory (IAA no. 70RCSA20K00000044), Pacific Northwest National Laboratory (IAA no. 70RCSA20K00000045) and Systems Planning and Analysis, Inc. (IAA no. FNNR-23-00010).[a]

Grant of License

The Contractor grants to the government, and others acting on its behalf, a nonexclusive, paid-up, irrevocable, world-wide license in such copyrighted data to reproduce, prepare derivative works, distribute copies to the public, and perform publicly and display publicly, by or on behalf of the government.

Please be aware that the acknowledgements or citations included in this manuscript are not intended as either an advertisement or government sponsorship for the services or entities listed.

References

[1] Cybersecurity and Infrastructure Security Agency, "National Critical Functions," [Online]. Available: https://www.cisa.gov/topics/risk-management/national-critical-functions. [Accessed March 2024].

[2] Cybersecurity and Infrastructure Security Agency, "Critical Infrastucture Sectors," [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/critical-infrastructure-sectors. [Accessed March 2024].

[3] Cybersecurity and Infrastructure Security Agency, "National Infrastructure Protection Plan and Resources," 2013. [Online]. Available: https://www.cisa.gov/topics/critical-infrastructure-security-and-resilience/national-infrastructure-protection-plan-and-resources. [Accessed March 2024].

[a] The underlying research discussed in this paper was further supported by the following organizations: Argonne National Laboratory, Idaho National Laboratory, Lawrence Livermore National Laboratory, and Los Alamos National Laboratory.

[4] B. Kolasky, "Status Update on the National Critical Functions," U.S. Department of Homeland Security Cybersecurity & Infrastructure Security Agency National Risk Management Center, 2021.

[5] J. Reinhardt, M. Secor, L. Miles, R. Lafond, D. Koolman II, L. Wind, L. Ludwig and J. Munns, "A Risk Assessment and Reduction Approach for National Critical Infrastructure," *Probabilistic Safety Assessment and Management PSAM 16,* pp. 1-12, 2022.

[6] S. Guikema and P. Gardoni, "Reliability Estimation for Networks of Reinforced Concrete Bridges," *Journal of Infrastructure Systems,* vol. 15, no. 2, pp. 61-69, 2009.

[7] R. Guldotti, V. Chmelewski, V. Unnikrishnan, P. Gardoni, T. McAllister and J. van de Lindt, "Modeling the Resilience of Critical Infrastructure: The Role of Network Dependencies," *Sustainable and Resilient Infrastructure,* vol. 1, no. 3-4, pp. 153-168, 2016.

[8] P. Ganguly and S. Mukherjee, "A Simulation-Based Generalized Framework to Model Vulnerability of Interdependent Critical Infrastructure Systems Under Incomplete Information," *Computer-Aided Civil and Infrastructure Engineering,* vol. 38, no. 18, pp. 2637-2559, 2023.

[9] J. Johansson and H. Hassel, "An Approach for Modelling Interdependent Infrastructures in the Context of Vulnerability Analysis," *Reliability Engineering & System Safety,* vol. 95, no. 12, pp. 1335-1344, 2010.

[10] J. Lindstrom and J. Johansson, "Towards Conceptualizing and Modelling Critical Flows- A Three-Tier Modelling Framework with a Swedish Example," in *Probablisitic Safety Assessment and Management, PSAM*, Honolulu, HI, 2022.

[11] J. L. Manefjord and J. Johansson, "Critical Flows Throughout the Covid-19 Pandemic- A Longitudinal Study on Interdependencies and Resilence in a Swedish Context," *International Journal of Disaster Risk Reduction,* vol. 103, 2024.

[12] A. Dekker, "Simulating Network Robustness for Critical Infrastructure Networks," *Proceedings of the 28th Australasian Conference on Computer Science,* vol. 38, pp. 59-67, 2005.

[13] Y. Fang, N. Pedroni and E. Zio, "Resilience-Based Component Importance Measures for Critical Infrastructure Network Systems," *IEEE Transactions on Reliability,* vol. 65, no. 2, pp. 502-512, 2016.

[14] J. Gero and U. Kannengiesser, "A Function-Behavior-Structure Ontology of Processes," *Artificial Intelligence for Engineering and Design, Analysis, and Manufacturing,* vol. 21, pp. 379-391, 2007.

[15] S. M. Rinaldi, J. P. Peerenboom and T. K. Kelly, "Identifying, understanding, and analyzing critical infrastructure interdependencies," *IEE Control Systems Magazine,* vol. 21, no. 6, 2001.

[16] A. L. Barabasi, *Network Science,* Cambridge University Press, 2016, p. 475.

[17] S. Chatterjee, A. Ganguly, D. Thomas, M. Oster, T. Fujimoto and S. Mahserejian, "A Network of Networks Framework for Analyzing Functions-Based Critical Infrastructure Risk and Resilence," in *Invited Talk at the Society for Risk Analysis Annual Meeting*, Tampa, FL, 2022.

[18] J. Watson, S. Chatterjee and A. Ganguly, "Resilience of Urban Rail Transit Networks Under Compound Natural and Opportunistic Failures," in *IEEE International Symposium on Technologies for Homeland Security*, Boston, MA, 2022.

[19] M. Oster, A. Ganguly, D. Thomas, D. Corbiani, J. Webster, F. Pan, B. Gattis and K. Kaynie, "A Tri-Level Optimization Model for Interdependent Infrastructure Network Resilience Against Compound Hazard Events," in *IEEE International Symposium on Technologies for Homeland Security*, Boston, MA, 2021.

[20] U.S. Department of Homeland Security, "DHS Risk Lexicon," 2010. [Online]. Available: https://www.cisa.gov/sites/default/files/publications/dhs-risk-lexicon-2010_0.pdf. . [Accessed 3 April 2024].

[21] U.S. National Academies, "Disaster Resilience: A National Imperative," 2012. [Online]. Available: https://nap.nationalacademies.org/catalog/13457/disaster-resilience-a-national-imperative. [Accessed 3 April 2024].

[22] U.S. Department of Homeland Security Cybersecurity and Infrastructure Security, "Infrastructure Data Taxonomy," [Online]. Available: https://www.cisa.gov/resources-tools/resources/infrastructure-data-taxonomy.