Analytics for Cybersecurity Policy of Cyber-Physical Systems

Nazli Choucri

Professor
Political Science Department
Massachusetts Institute of Technology

Gaurav Agarwal

Independent Contractor
Massachusetts Institute of Technology

November 14, 2022

Abstract

Guidelines, directives, and policy statements are usually presented in "linear" text form—word after word, page after page. However necessary, this practice impedes full understanding, obscures feedback dynamics, hides mutual dependencies and cascading effects and the like—even when augmented with tables and diagrams. The net result is often a checklist response as an end in itself. All this creates barriers to intended realization of guidelines and undermines potential effectiveness. We present a solution strategy using text as "data", transforming text into a structured model, and generate network views of the text(s), that we then can use for vulnerability mapping, risk assessments, and control point analysis. For proof of concept, we draw on NIST conceptual model and analysis of guidelines for smart grid cybersecurity, more than 600 pages of text.

Keywords

Cyber-physical systems, cybersecurity, NISTIR 7628 Rev.1, smart grid, design structure matrix, network view.

Citation: Choucri, N., & Agarwal, G. (2022). Analytics for cybersecurity policy of cyber-physical systems. *Proceedings of the 2022 IEEE International Symposium on Technologies for Homeland Security* (HST).

Unique Resource Identifier: https://hdl.handle.net/1721.1/146916

Version: Author's final manuscript.

Acknowledgement: This material is based on work supported by the U.S. Department of Defense for National Security Agency, *Science of Security & Privacy Program* under Grant No. H98230-18-D-00-0010. Any opinions, findings, conclusions or recommendations therein are those of the author(s) and do not necessarily reflect the views of the US Department of Defense.

Analytics for Cybersecurity Policy of Cyber-Physical Systems

Nazli Choucri
Professor of Political Science
Massachusetts Institute of Technology
Cambridge, MA, USA
nchoucri@mit.edu

Gaurav Agarwal
Independent Contractor
Massachusetts Institute of Technology
Cambridge, MA, USA
gauravag@mit.edu

***Abstract*— Guidelines, directives, and policy statements are usually presented in "linear" text form—word after word, page after page. However necessary, this practice impedes full understanding, obscures feedback dynamics, hides mutual dependencies and cascading effects and the like—even when augmented with tables and diagrams. The net result is often a checklist response as an end in itself. All this creates barriers to intended realization of guidelines and undermines potential effectiveness. We present a solution strategy using text as "data", transforming text into a structured model, and generate network views of the text(s), that we then can use for vulnerability mapping, risk assessments, and control point analysis. For proof of concept, we draw on NIST conceptual model and analysis of guidelines for smart grid cybersecurity, more than 600 pages of text.**

Keywords—cyber-physical systems, cybersecurity, NISTIR 7628 Rev.1, smart grid, design structure matrix, network view

I. INTRODUCTION

As general practice, guidelines, directives, and policy documents are presented in text form, page-by-page and word-by-word—supported with figures, diagrams and tables as needed. Rooted in the legal tradition, this practice reinforces a linear logic, on in which where sequence appears to dominate.

A. Problem

Cybersecurity policies are developing faster than their implementation. Barriers to implementation reduce the value of policies to protect systems (and users) from known vulnerabilities.

The cybersecurity policy ecosystem is complex: Enterprises are burdened by the need to identify and situate required directives. Policies are usually articulated in text form, as are descriptions of system-state. Text creates ambiguity for precise representation of a system as well as for accurate identification of vulnerabilities and impacts.

Such a situation creates a dilemma for implementing *what* is to be done, *why, when, where*. By definition, text undermines any attention to feedback, delays, interconnections, cascading effects, indirect impacts and the like—all embedded deep into the idiom or structure of the textual form. The text-form may be necessary, but it is not sufficient. In fact, it may impede understanding, obscure the full nature of directives, and generate less than optimal results—all of which create impediments to the pursuit of effective outcomes.

B. Purpose

This paper presents a solution strategy that consists of deploying analytical tools to formal text for the purpose of capturing as much of the features and intents of policies and guidelines as possible.

Focusing on the salience of cybersecurity in both private and public sectors, we draw on major reports presented by the National Institute for Standards and Technology (NIST) [1, 2] in its efforts to improve cybersecurity. These reports provide analyses of system-state, risk assessments, probability metrics, as well as detailed annotations to help guide the user community.

In sum, this material is rich in content, based on considerable collective knowledge, and subjected to a careful scrutiny and evaluation.

C. Proof of Concept

This paper presents a proof of concept for our approach to *analytics for cybersecurity policy of cyber-physical systems* as well as operational methods to:

- Transend constraints of policy-as-text or system-as-text;
- Transform text into metrics;
- Use metrics to construct model of system-state (for the test case) based on system metrics;
- Create effective linkages among required policy directives for cybersecurity;
- Connect model of system-state to directives for implementation; and
- Target specific directive to specific system problem-point.

Specifically, the proof of concept focuses on the smart grid of electric power systems. Among the daunting challenges is that directives—for implementation of cybersecurity policy—

This material is based on work supported by the U.S. Department of Defense for National Security Agency, Science of Security & Privacy Program under Grant No. H98230-18-D-00-0010. Any opinions, findings, conclusions, or recommendations therein are those of the author(s) and do not necessarily reflect the views of the US Department of Defense.

are distributed across a policy ecosystem of multiple documents. The policy ecosystem must be created before any of the above noted operational steps are undertaken. In practice this generally means that we have to identify and consider all properties of the cyber-physical system, of the policy directives, and of their connections.

D. Products

The expected result is a modular but integrated approach to policy recommendations that (i) efficiently conveys policy prescriptions within an organization [3]. [4–5], (ii) provide different visual structures for "seeing" cyber policy strategies, and (iii) situate attendant trade-offs or limitation in framing strategies for cyber policy.

II. Research Design

A. Design Overview

The research design, presented below, is in five steps and at a relatively high level of aggregation.

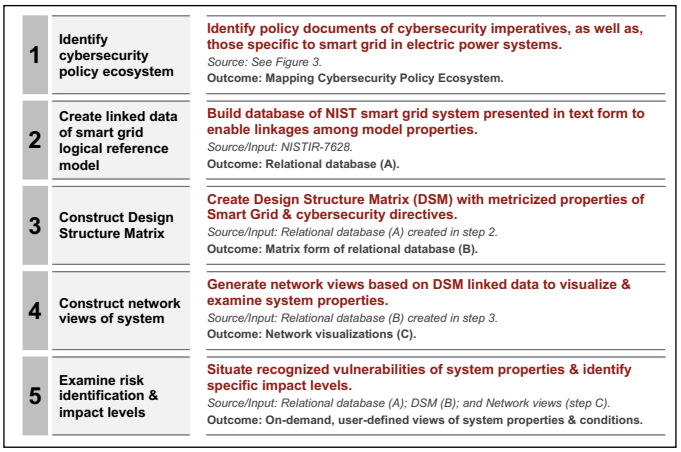

Fig. 1. High-level overview of research design.

To briefly note the steps in Fig. 1:

1) Identify Policy Ecosystem: The first step is to identify the policy ecosystem for cybersecurity, and to delineate the focus of analysis. Once the policy ecosystem is completed and partitioned for inquiry, then we turn to operational features of the research design. Here, we apply the structured method (Fig. 2) to assist understanding of *guidelines for smart grid cybersecurity* as provided in NISTIR 7628 [6].

2) Create Linked Data: We view the smart grid logical reference model provided in NISTIR 7628 [6] more as a synthesis of empirical evidence and examine its properties accordingly. By drawing on these documents we transform the basic text into a formal model of the entire system for the proof of concept (that is, the NIST "smart grid logical reference model").

3) Construct Design Structure Matrix (DSM) The *linked data* are converted into a DSM [7-8] for matrix-based analysis. The full DSM allows us to "dig in deeper" or to focus in some segment thereof, as we show later on. *Linked data* are also used in the form of interactive tool(s) for on-demand, user-defined views of system properties. Such tools allow us to examine parts and pieces of the DSM for: (i) exploratory analyses of the smart grid system and (ii) drill down analyses of the same data set.

4) Construct Network Graphics: the Design Structure Matrix is then transformed into smart grid network graphics of the system as a whole and the connections among components. The network graphics capability is supported by data visualization and analysis tools.

5) Risk identification & Assessment: All the above steps support the practice of cybersecurity risk management as well as the use of NIST Cybersecurity Framework [9] for enterprise purposes and customized to system operations.

Jointly, these tools assist users to address questions related to the *what, when, where, who, why, how and how much* for system cybersecurity, as well as questions related risks/vulnerabilities. For example, what are the cybersecurity requirements are applicable to a specific interface between two actors and with what impact levels?

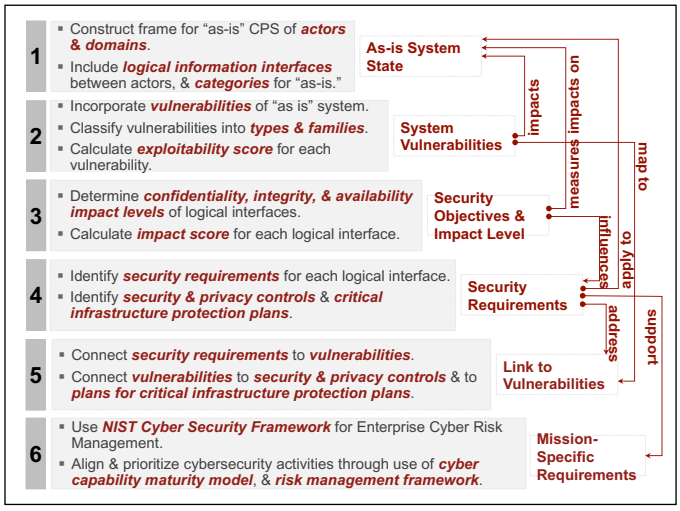

Fig. 2. High-level view of structured method for policy analysis of cybersecurity for a cyber-physical system.

III. Policy Ecosystem

There is little need for introduction of NIST, the premier standard setting entity in the nation and often for the international community as a whole.

In this study, we go beyond appreciating the contributions of NIST to viewing reports as a source of new knowledge, a basis for identifying risk, evaluating alternative courses of action, and facilitating prioritization in the deployment of corrective measures.

Fig. 3 shows the results of the policy ecosystem relevant to the proof of concept and the scope of this investigation. The yellow shade identifies the policy documents that bear directly on this study.

A. Proof of Concept: Smart Grid for Electric Power Systems

Our focus of this study is smart grid—a ubiquitous feature of power systems—and its cybersecurity. We use the NISTIR 7628 [6] on *guidelines for smart grid cybersecurity*—totaling

more than 600 pages—from the overall NIST ecosystem as the basis to create our linked data and conduct our investigations.

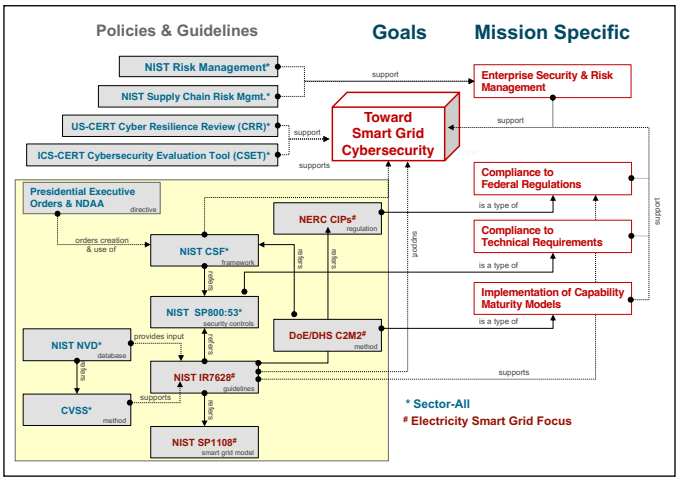

Fig. 3. Smart grid cybersecurity policy ecosystem.

B. *NISTIR 7628: Guidelines for smart grid cybersecurity*

While NISTIR 7628 [6] contains almost all of the relevant information required to (i) map the smart grid security requirements for purposes of technical operations, business strategy and technology policy, and (ii) address the key challenges identified by GAO[1] [10] and [11–14], however as a voluntary guideline it has the following limitations:

- NISTIR 7628 [6] is a comprehensive and very detailed record of the elements of smart grid that assist in the standard and agenda setting. But information is all text and distributed across a very large document.
- It may be a daunting challenge to fully understand the very detailed and often unfamiliar information in a report presented in three disparate volumes and focusing on technology, privacy, and IT security.
- The document itself refers to other documents that provide detailed information on a conceptual smart grid, its actors and activities, interfaces between actors, and their attributes – all in text form.
- The report does not allow extraction of information at different levels of abstraction due to the disconnected nature of the content adding further burden to anyone seeking to synthesize the content.
- So, too, the current form does not connect and address to the business objectives and organizational policies. It cannot be mapped to the technology policy and business strategy requirements due to highly technical nature of the content without relying on external literature for an end-to-end system view of cyber security.

While the report provides a detailed account of the elements of the smart grid and possible scenarios of failures, it does not provide any mapping to actors and interfaces involved in smart grid functions. Thus, limiting the ability to:

- Locate control points; and
- Measure current and future desired state of the technical landscape, business objectives and technology policy.

IV. Linked Data

Using the NIST logical reference model provided in NISTIR 7628 [6] as an entry point, following critical data are extracted to define the elements of the linked database. The consist of six distinct system properties, as follows:

1) Actor "...is a device, computer system, software program, or the individual or organization that participates in the smart grid [6]". NISTIR 7628 [6] identified 49 such actors that are clustered into seven domains based on their role and responsibilities at the macro level.

2) Domains encompass smart grid conceptual roles and services. These include types of services, interactions, and stakeholders that make decisions and exchange information necessary for performing identified goals.

3) Logical Interfaces connect any two actors. NISTIR 7628 [6] identified over 125 such interfaces between 49 actors. These interfaces are further aggregated tinto 22 *Logical Interface Categories* based on their technical requirements.

4) Impact Levels: Three levels of impact (low, moderate, high) are defined as the expected adverse effect of a security breach on system operations, system assets, or individuals for each *security objective* (confidentiality [2], integrity [3], and availability[4]) as defined in US statute 44 U.S.C., Sec. 3542 [15].

5) Security Requirements are applicable to any logical interface, based on impact level for each security objective. They are an amalgam located in different sources sources, notably: NIST SP 800-53 [16], the DHS Catalog [17], and NERC CIP (Critical Infrastructure Plans) standards [18]. These requirements are organized into families primarily based on NIST SP 800-53 [16] and are allocated to one of three categories (a–c) below:

a) Governance, Risk, and Compliance Requirements that are addressed at organizational level. They are centered around policy, procedure, and compliance-based activities.

b) Common Technical Requirements that are applicable to all the logical interface categories.

[1] GAO [10] identified six key challenges: (i) Aspects of the regulatory environment may make it difficult to ensure smart grid systems' cybersecurity; (ii) Utilities are focusing on regulatory compliance instead of comprehensive security; (iii) The electric industry does not have an effective mechanism for sharing information on cybersecurity; (iv) Consumers are not adequately informed about the benefits, costs, and risks associated with smart grid systems; (v) There is a lack of security features being built into certain smart grid systems; and. (vi) The electricity industry does not have metrics for evaluating cybersecurity.

[2] Confidentiality is defined as "*…preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information* [15]."

[3] Integrity is defined as *"…guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity* [15]."

[4] Availability is defined as *"…Ensuring timely and reliable access to and use of information* [15]."

c) Unique Technical Requirements that are allocated to one or more of the logical interface categories.

6) System Vulnerabilities: Weaknesses which could adversely impact the operation of the electric grid that are categorized into people, policy, and procedure; platform software/firmware vulnerabilities; platform vulnerabilities; and network factors.

Fig. 4 provides a high-level view of the data collected from the NISTIR 7628 [6]. This figure shows not only the value of the document, but the challenges for the reader to extract the relevant data and understand how sets of data are related to each other.

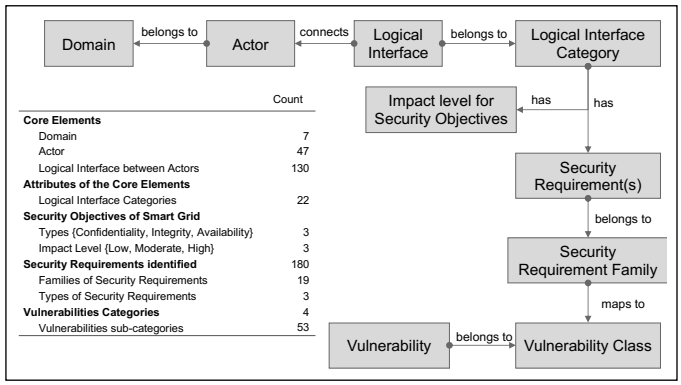

Fig. 4. Operational view of linked data extracted from NISTIR 7628 [6]. *Inset*: Individual count of observations within each data element.

V. Design Stucture Matrix (DSM)

DSM is an important venue for quantitative analysis [7-8, 19]. It is a matrix-based information exchange tool for representing interactions between the elements or activities of a decomposed system.

The actors and logical interfaces in Fig. 4 from NISTIR 7628 [6] are converted into a DSM (Fig. 5). By linking added information on impact levels and security requirements, DSM view helps to identify which actor or cluster of actors is more important than others. Such a view may help us to identify and understand where most of the effort is needed.

Actor Name	Actor	1	2	3	4	5	6	7	8	9	10	11	12	13	15	16	17	18	19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	36	37	38	39	40	48	49	41	42	43	44	45	46	47
Plant Control System –Distributed Control System	1	1	Generation																																													
Customer	2		2								U127		Customer										U125	U40																											
Customer Appliances andEquipment	3			3		U44		U43	U120		U129																																					
Customer Distributed Energy Resources: Generation and Storag	4				4	U45		U130			U48																																					
Customer EnergyManagement System	5			U44	U45	5	U62	U42	U41	U126	U46												U119				U88					U106											U92		U95				
Plug-in Electric Vehicle/ Electric Vehicle Service Element	6					U62	6	U49			U50																																					
Home Area NetworkGateway	7			U43	U130	U42	U49	7	U60	U124	Ux5	U128									U25							U59			U32		U54											U18			
Meter	8			U120		U41		U60	8		U47					U35					U24																					U64					
Customer Premise Display	9		U127			U126		U124		9																																						
Sub-Meter – Energy UsageMetering Device	10			U129	U48	U46	U50	Ux5	U47		10																																					
Water/Gas Metering	11							U128				11																																				
Distribution Data Collector	12												12		U112			U111	Distribution																								U133						
Distributed IntelligenceCapabilities	13													13	U108																																	
Distribution Remote Terminal Unit/Intelligent Electronic Device	15												U112	U108	15						U3				U137	U109			U117						U67												
Field Crew Tools	16								U35							16	U105					U14				U104	U99							U29			U34									
Geographic InformationSystem	17															U105	17					U110				U102												U131	U133							
Distribution Sensor	18												U111					18																														
Energy MarketClearinghouse	19																		19	U17	Markets						U97												U133		U20						
Independent System Operator/Regional Transmission Organiza	20																		U17	20									U72	U90												U93						
Advanced MeteringInfrastructure Headend	21							U25	U24						U3						21		U21			U7				U22	U2		U26					U133			U98		U6			
Bulk Storage Management	22																					22								U66					Ux3							Operations						
Customer InformationSystem	23		U125			U119										U14	U110				U21		23	U38			U113				U33					U37		U31	U133			U96					
Customer ServiceRepresentative	24		U40																				U38	24															U133								
Distributed Generation andStorage Management	25														U137										25				U65	Ux2																
Distribution Engineering	26														U109											26	U114																				
Distribution ManagementSystems	27					U88										U104	U102		U97		U7		U113		U114	27	U101	U9	U87		U11	U8		U10		U12				U15						
Distribution Operator	28															U99										U101	28	U100																		
Distribution SupervisoryControl and Data Acquisition	29							U59							U117				U57					U65		U9	U100	29		U56		U55	U27	U115							U51	U63					
Energy Management System	30	U74																		U72				Ux2		U87			30	U89				U83		U77					U91						
ISO/RTO Operations	31	U70																	U58	U90		U66						U56	U89	31					U116		U78				U52	Ux6		U134			
Load Management Systems/Demand Response Management S	32					U106		U32													U22		U33			U11					32				U13			U36								
Meter Data ManagementSystem	33																				U2					U8						33									U1		U5			
Metering/Billing/Utility BackOffice	34							U54																					U55				34				U133			U53	Ux4					
Outage Management System	36															U29					U26								U27					36			U30									
Transmission SCADA	37	U80													U67							Ux3				U10			U115	U83	U116	U13				37		U75					U85	U81	U82
Customer Portal	38		U39																				U37													38			U133						
Wide Area MeasurementSystem	39																													U77	U78					U75		39					U79		
Work Management System	40															U34	U131						U31			U12												40							
Security/Network/SystemManagement	48												U133				U133		U133		U133		U133	U133										U133			U133			48		U133	U133	U133	U133			
Transmission Engineering	49																																								49					U135	U136	
Aggregator/Retail EnergyProvider	41					U92													U20	U93							U15		U51	U91	U52			U53					U133		41	U4	Service Providers				
Billing	42								U64												U98		U96						U63		Ux6		U1	Ux4					U133		U4	42					
Energy Service Provider	43					U95																																	U133				43				
Third Party	44							U18													U6												U5						U133					44			
Phasor Measurement Unit	45																													U134					U85		U79							45		
Transmission IntelligentElectronic Device (IED)	46																																		U81					U135		Trasnmission			46	
Transmission RemoteTerminal Unit (RTU)	47																																		U82					U136						47

Fig. 5. Design structure matrix of NIST smart grid reference model.
Note: Logical interface, indicated by a number in the cell at the intersection of row and column, connects the *row*-actor to the *column*-actor.

VI. Network Views

Information provided in matrix form (Fig. 5) and in *linked data* (Fig. 4) is useful in its basic form, however its value can be further enhanced if it can be visualized and analyzed holistically at the systems level.

With the foundations in place the next step is to transform the DSM (Fig. 5) into network graphics supported by visualization/analysis tool(s).

The combination of graph theory and its underlying tools help transform the DSM into very informative and valuable Cumulatively these tools aid user in answering questions related to *what, when, where, who, why, how, and how much* of smart grid functions and their cybersecurity and questions related to mitigation of cybersecurity risks/vulnerabilities: We as: which Cybersecurity Requirements are applicable to an interface between two actors at what impact levels?

Using the DSM in Fig. 5, we create a visual representation of the smart grid network (Fig. 6). The results allow visual interpretation of the structure by turning structural proximities into visual proximities, thus facilitating analysis.

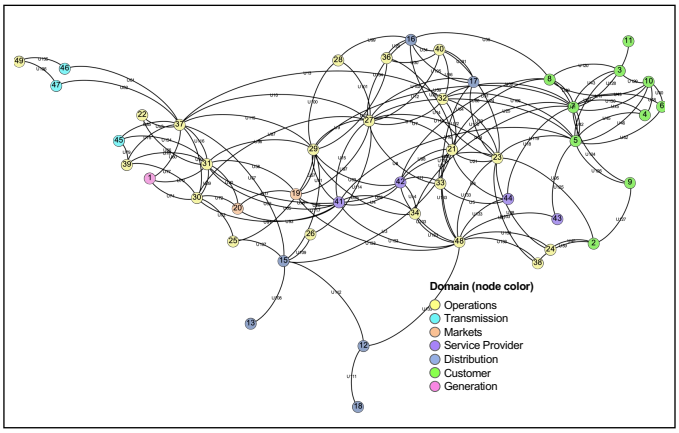

Fig. 6. Network view of NIST smart grid reference model. *Note*: Nodes represent actors and an edge between any two nodes represents the logical interface between them, node color indicates domain of actor. This view is based on a force directed layout [20], where nodes repulse each other like charged particles, while edges attract their nodes, like springs. The force-directed layout drawing has the specificity of placing each node in a situation depending on the other nodes. This process depends only on connections between nodes.

VII. Risk Identification & Assessment

So far, we focused on retrieving the knowledge embedded in the text and, as needed.

The next set of steps focus on matters of risk (Step 5 of Fig. 1), i.e., to examine the structure of the network and focus on those elements (actors/activities and interface between any two such actors/activities) for risk assessments that are central to the user's interests, and, to meet the statutory requirements for cybersecurity, for example, implementing NIST Cyber Security Framework [9].

A. Comparative Analysis of Nodes

The core network view can be used to create additional views by resizing nodes by node/actor centrality measures [21–22] as follows:

1) Eigenvector centrality: Importance of a node in the network based on the coupling with other high-ranking neighboring nodes.

2) Betweenness Centrality: Focus on how important a node is in terms of connecting other nodes.

3) Closeness Centrality: Focus on how easily other nodes can reach a node.

4) Closeness Centrality: Degree Centrality: Measures how a node is connected to others.

For this paper, we use eigenvector centrality, where node centrality is determined by the centrality of its neighbors. It is not node centrality itself that matters, it is the centrality of the nodes linked to it. The circularity of the argument is evident but can understood using matrix algebra [28].

B. Comparative Analysis Based on Impact Level

The information provided in the NISTIR 7628 [6] report is then compiled for the impact of any risk/vulnerability on the interfaces between any two actors/activities of the smart grid for three key security objectives—Confidentiality, Integrity, Authority.

Edge color is used here to represent the impact level on the smart grid based on three security objectives.

C. Comparative Analysis Based on Security Requirements

Next, the edge width is resized based on the count of security requirements to secure the logical interface. recommended for each of the three security objectives and impact levels.

Fig. 7 presents the 3x3 view of impact level (low, moderate, high) and *count of security requirements* for all three security objectives throughout the network. All the visuals in Fig. 7 are based on exactly the same data or information, but they differ considerably in explanatory value.

Of course, the network views are possible only because of the NIST conceptual view that helps direct the analysis to the relevant supporting tables so essential for building the DSM.

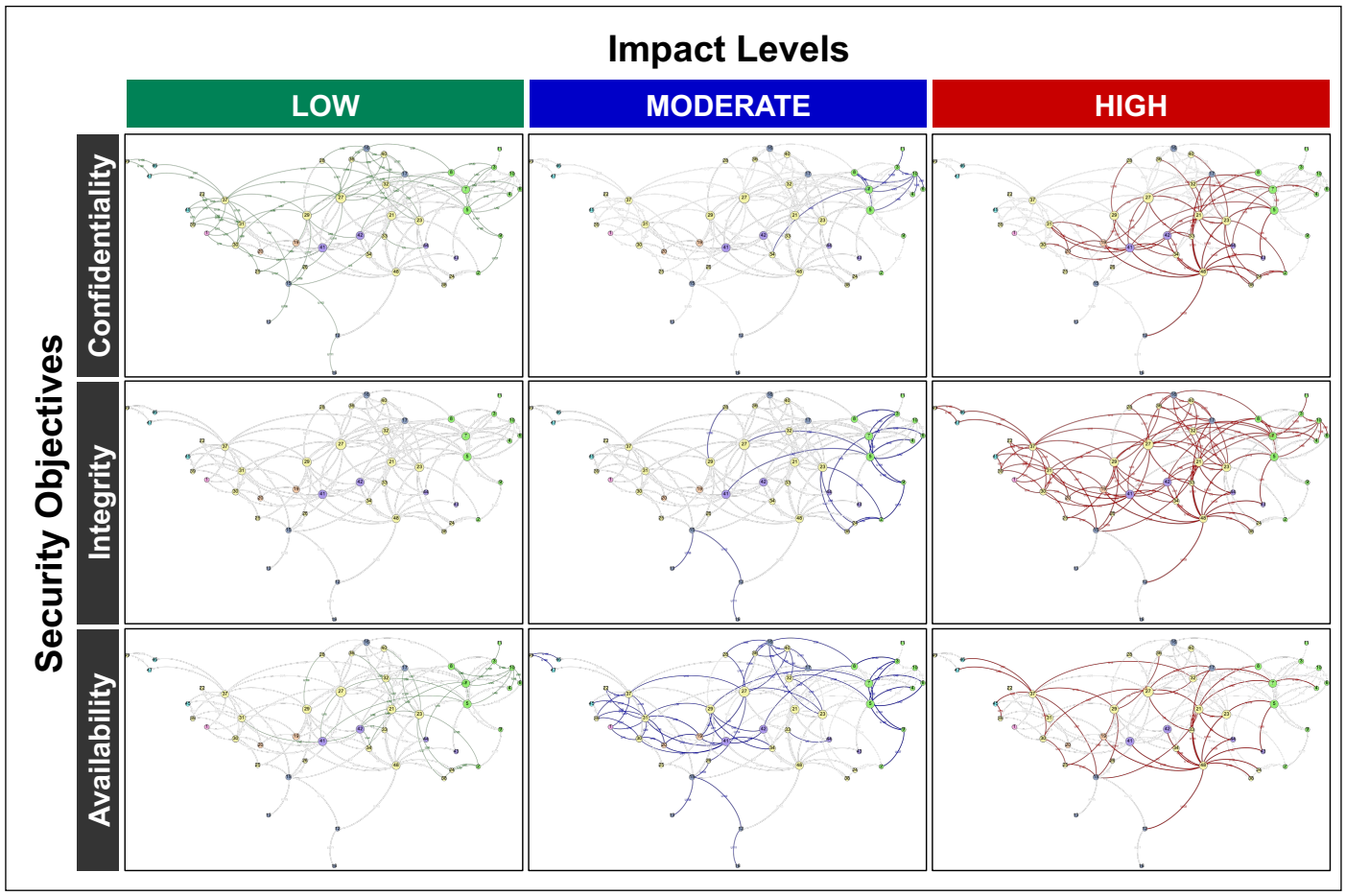

Fig 7. Security Objectives by by Impact Level (high, medium, low) in 3x3 views of NIST smart grid reference model.
Note: Node size indicates eigen vector centrality of node; node color indicates domain of actor, see legend in Fig. 6; only select edges—relevant to a security objective at select impact level—are highlighted; edge width indicate count of security requirements—relevant to a security objective at select impact level.

D. Consolidating 3x3 Views

While the information in Fig. 7 is of direct relevance to the user or enterprise, it is not particularly useful for operational purposes. The figure is too detailed to facilitate effective action. Further it serves as a disincentive to action. Of course, the user can "drill down" or "zoom in" to examine further.

We now aggregate the information in 3x3 to a single image by selecting the worst impact level for a logical interface (represented by the edge color) and *aggregating the count* of security requirements (represented by edge width) in Fig. 8.

E. Tools for N-x Contingency Analysis

This paper addresses N-1 vulnerabilities, i.e., analysis of vulnerabilities is limited to node or edge. However, analysis of second and higher degrees of impact on the network and who else may be impacted should the actors or logical interface fail or are compromised will help in reviewing the other components that need to secure to limit the loss.

The network structure and matrix representation enable analysis of multiple vulnerabilities or multiple "N-x" levels of vulnerabilities to be analyzed It has the capability for exploring how vulnerability in one node or edge impacts resources beyond its means or privileges. It identifies the second degree of impact

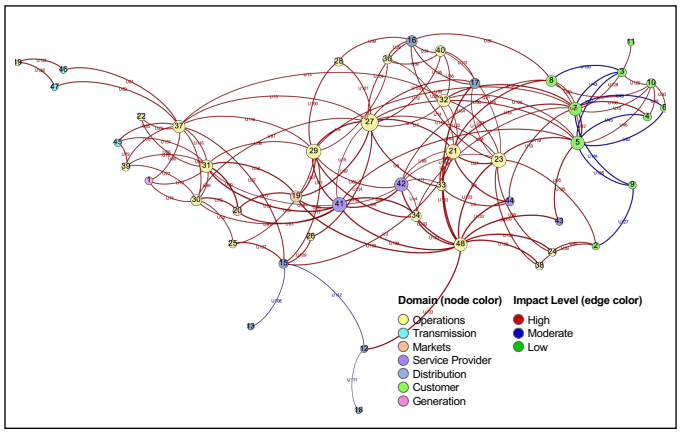

Fig. 8. Consolidated network view of NIST smart grid reference model. *Note*: Nodes represent actors, node color indicates domain of actor, node size indicates eigen vector centrality of node; and edge between any two nodes represents the logical interface between them.

that the network may have and who else may be impacted should the actors or logical interface fails/compromised. This will help in reviewing the other components of the system that need to be secured to limit loss.

VIII. Enterprise Application

If an enterprise uses our method of *linked database* and seeks to customize the results for its own system properties, then it must incorporate its own enterprise-specific knowledge into the essential structure of cybersecurity directives. This means that an enterprise must:

A. Map its own system to NIST "as-is" system

Given that our work is based on a sector independent framework and guideline documents, any enterprise that uses the method will need to map its own system components and policies to the relevant reference documents.

B. Identify system specific vulnerabilities

Based on enterprise mapping, an enterprise will also need to develop an assessment of the threat landscape, as well as the vulnerabilities identified, and known by, the system owners.

In conclusion, we believe that the methods we developed, and the tools provided, would greatly facilitate the tasks of the enterprise as it seeks to comply with security guidelines.

References

[1] *NIST. Cybersecurity*, Accessed: Oct. 10, 2022. [Webpage]. Available: https://www.nist.gov/cybersecurity

[2] Y. Wang et al., "Analysis of smart grid security standards," in *2011 IEEE International Conference on Computer Science and Automation Engineering*, Shanghai, pp. 697–701, 2011, doi: 10.1109/CSAE.2011.5952941.

[3] T. Herath, and H. R. Rao, "Encouraging information security behaviors in organizations: Role of penalties and perceived effectiveness," *Decision Support Systems*, vol. 47, pp. 154–165, 2009, doi: 10.1016/j.dss.2009.02.005

[4] J. Stoll, and R. Z. Bengez, "Visual structures for seeing cyber policy strategies", in *2015 7th International Conference on Cyber Conflict: Architectures in Cyberspace*, pp. 135–152, 2015, doi: 10.1109/CYCON.2015.7158474.

[5] M. Harvey, D. Long, and K. Reinhard, "Visualizing NISTIR 7628, guidelines for smart grid cyber security," in *2014 Power and Energy Conference at Illinois (PECI)*, Champaign, IL, pp. 1–8, 2014, doi: 10.1109/PECI.2014.6804566.

[6] A. Lee, *Guidelines for Smart Grid Cyber Security, NIST Interagency/Internal Report (NISTIR)*. Gaithersburg, MD: National Institute of Standards and Technology, 2010, doi: 10.6028/NIST.IR.7628.

[7] T. R. Browning, "Design Structure Matrix Extensions and Innovations: A Survey and New Opportunities," in *IEEE Transactions on Engineering Management*, vol. 63, no. 1, pp. 27–52, Feb. 2016, doi: 10.1109/TEM.2015.2491283.

[8] T. R. Browning, "Applying the design structure matrix to system decomposition and integration problems: a review and new directions," in *IEEE Transactions on Engineering Management*, vol. 48, no. 3, pp. 292-306, Aug 2001, doi: 10.1109/17.946528.

[9] M. Barrett, *Framework for Improving Critical Infrastructure Cybersecurity Version 1.1*, NIST Cybersecurity Framework, 2018, doi: 10.6028/NIST.CSWP.04162018.

[10] United States Government Accountability Office, "Electricity grid modernization," *Report to Congressional Requesters*, no. AO-11-117, January 2011. [Online]. Available: https://www.gao.gov/assets/gao-11-117.pdf.

[11] R. K. Abercrombie, F. T. Sheldon, K. R. Hauser, M. W. Lantzand, and A. Mili, "Risk assessment methodology based on the NISTIR 7628 guidelines," in *2013 46th Hawaii International Conference on System Sciences*, Wailea, HI, USA, pp. 1802–1811, 2013, doi: 10.1109/HICSS.2013.466.

[12] A. C. F. Chanand, and J. Zhou, "On smart grid cybersecurity standardization: Issues of designing with NISTIR 7628," *IEEE Communications Magazine*, vol. 51, no. 1, pp. 58–65, January 2013, doi: 10.1109/MCOM.2013.6400439.

[13] M. Uslar, C. Rosinger, and S. Schlegel, "Security by design for the smart grid: Combining the SGAM and NISTIR 7628," in *2014 IEEE 38th International Computer Software and Applications Conference Workshops*, Vasteras, pp. 110–115, 2014, doi: 10.1109/COMPSACW.2014.23.

[14] A. Srivastava, T. Morris, T. Ernster, C. Vellaithurai, S. Pan, and U. Adhikari, "Modeling cyber-physical vulnerability of the smart grid with incomplete information," *IEEE Transactions on Smart Grid*, vol. 4, no. 1, pp. 235–244, March 2013, doi: 10.1109/TSG.2012.2232318.

[15] U.S. Government Publishing Office, "Definitions," *United States Code (2011 Edition)*, title 44, chapter 35, subchapter III, sec. 3542, 2011. [Online]. Available: https://www.govinfo.gov/content/pkg/USCODE-2011-title44/html/USCODE-2011-title44-chap35-subchapIII-sec3542.htm

[16] Joint Task Force Transformation Initiative, "Security and Privacy Controls for Federal Information Systems and Organizations," *NIST Special Publication*, no. 800-53, rev. 4, April 2013 (updated January 2015), doi: 10.6028/NIST.SP.800-53r4.

[17] National Cyber Security Division, "Catalog of control systems security: recommendations for standards developers," version 7. April 2011. [online]. Available: https://ics-cert.us-cert.gov/sites/default/files/documents/CatalogofRecommendationsVer7.pdf.

[18] North American Electric Reliability Corporation (NERC), "Reliability Standards: CIP (Critical Infrastructure Protection) Standards,", 2022. [Online]. Available: https://www.nerc.com/pa/Stand/Pages/ReliabilityStandards.aspx

[19] B. Rogers, and E. Gilbert, "Identifying architectural modularity in the smart grid: an application of design structure matrix methodology," in *Grid-Interop Forum*, Phoenix AZ, 2011. [Online]. Available: https://www.incose.org/docs/default-source/enchantment/130109_rogers-architecture-sgmodularityv2-presentation.pdf?sfvrsn=2

[20] M. Jacomy, T. Venturini, S. Heymann, and M. Bastian, "ForceAtlas2, a continuous graph layout algorithm for handy network visualization designed for the gephi software," *PLOS ONE*, vol. 9, no. 6, pp. e98679, 2014, doi: 10.1371/journal.pone.0098679.

[21] A. Ernster, and A. K. Srivastava, "Power system vulnerability analysis - towards validation of centrality measures," in *PES T&D 2012*, Orlando, FL, pp. 1–6, 2012, doi: 10.1109/TDC.2012.628148.

[22] L. De Benedictis, S. Nenci, G. Santoni, L. Tajoli, and C. Vicarelli, "Network analysis of world trade using the BACI-CEPII dataset," *CEPII Working Paper*, no. 2013-24, 2013. [online]. Available: http://www.cepii.fr/pdf_pub/wp/2013/wp2013-24.pdf.