Visualizing NISTIR 7628, Guidelines for Smart Grid Cyber Security

Matthew Harvey; Daniel Long; Karl Reinhard
University of Illinois Urbana-Champaign, Dept. of Electrical Engineering

***Abstract*— The National Institute of Standards and Technology Interagency Report (NISITR) 7628, *Guidelines for Smart Grid Cyber Security*, provides an analytical framework that stakeholders can use to develop effective Smart Grid related characteristics, risks, and vulnerabilities. NISTIR 7628 spans more than 600 pages and is densely packed with technical information drawn from multiple disciplines, which to many readers is difficult to broadly conceptualize and apply. This paper explores methods for visualizing the complexities of NISTIR 7628's cyber security guidelines for the nascent Smart Grid and aiding readers to better synthesize the information presented.**

I. Introduction

The United States and other advanced industrial countries around the world have embarked upon a long term effort to modernize their electric power infrastructures. This modernization effort includes applying advanced digital technologies to systems to expand communications and control over very large systems to achieve ever increasing efficiency while maintaining very high reliability. The broad application of digital technologies is accompanied by increased exposure to malicious attacks upon the power grid's digital infrastructures. As the digital infrastructure expands, the exposure to and consequences of compromise also expand.

In August of 2010, the National Institute of Standards and Technology (NIST) Computer Security Division published NISTIR 7628, *Guidelines for Smart Cyber Security*, which expands upon the Smart Grid cyber security principles published in NIST's 2010 Special Publication 1108, *NIST Framework and Roadmap for Smart Grid Interoperability Standards*. NISTIR 7628 synthesizes the input of more than 500 stakeholder representatives from the private sector (including utilities, vendors, manufacturers, and electric service providers), various standards organizations, academia, regulatory organizations, and federal agencies. The guidelines represent power, computer, information technology, and telecommunications industry perspectives. The document is a first effort to develop a technical, analytical framework needed to inform individuals and organizations responsible for addressing cyber security for Smart Grid systems and its constituent hardware and software components. The document is envisioned as a first step in evolutionary series of documents that will produce standard protocols, interfaces, and technical specifications needed for a secure Smart Grid. The document focuses exclusively on the cyber-security aspects and does not address physical security requirements.

II. NISTIR 7628

A. NISTIR Diagrams

NISTIR 7628 conceptualized the power grid at the higest level as being composed of seven Domains: **marketing, operations, sevice provider, bulk generation, transmission, distribution, and customer** as seen in Fig. 1. A Smart Grid domain is a high level grouping of orgainizations, buildings, individuals, systems, devices with similar objectives or functions.

Fig. 2 shows 46 actors that comprise the seven domains. Actors are devices, systems, or programs that make decisions and exchange the information necessary for the Smart Grid to function. This actors list is intended to be comprehensive, but not all inclusive, as this model represents diverse real-world organizations that are uniquely purposed and organized . The Logical Reference Model show in Fig. 3 depicts 130 logical interfaces (interactions between actors. The obvious challenge posed by this representation's complexity is for users to translate its high level abstractions into implementable policies and procedures on their organizations information processing systems (hardware, software, network, etc.)

To aid this synthesis, NISTIR 7628 identifies 22 logical

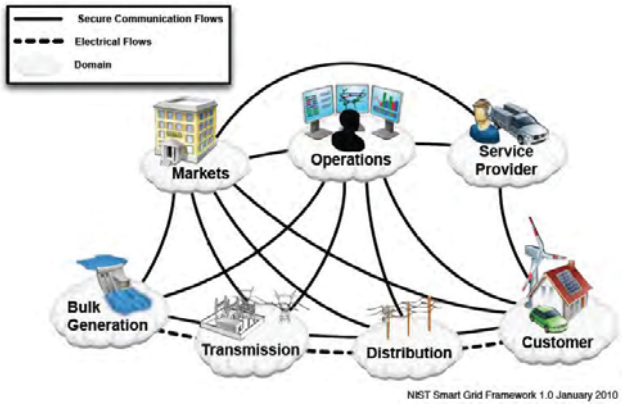

Fig. 1 Interactions of Actors in Different Smart Grid Domains through Secure Communications Flows [1]

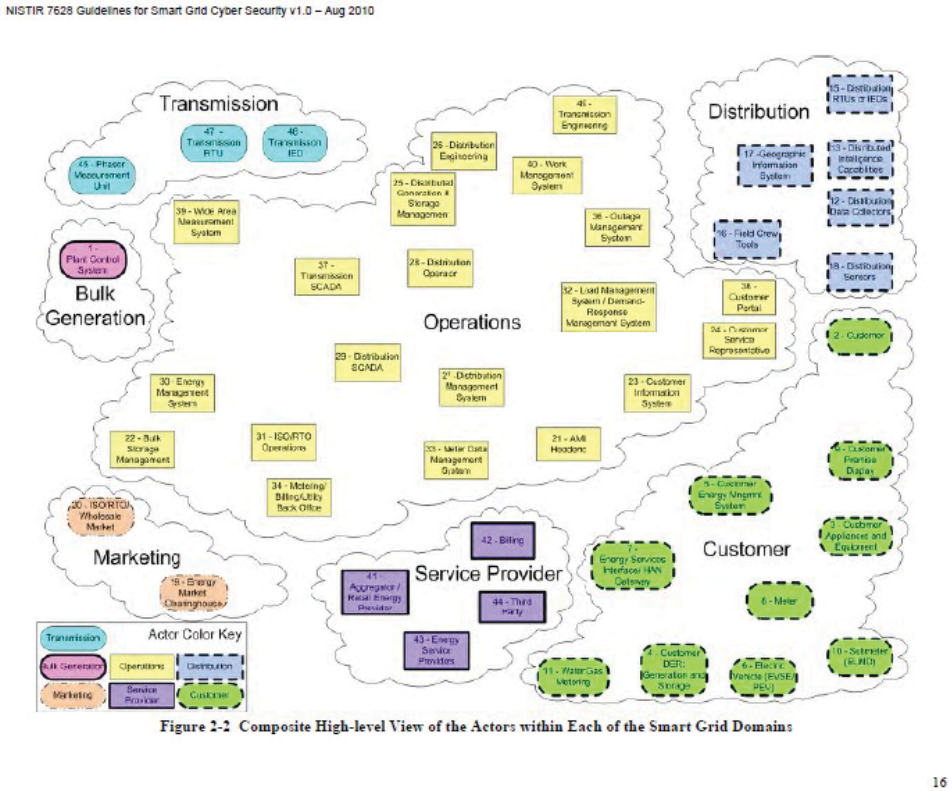

Fig. 2 Composite High-level View of the Actors within Each of the Smart Grid Domains [1]

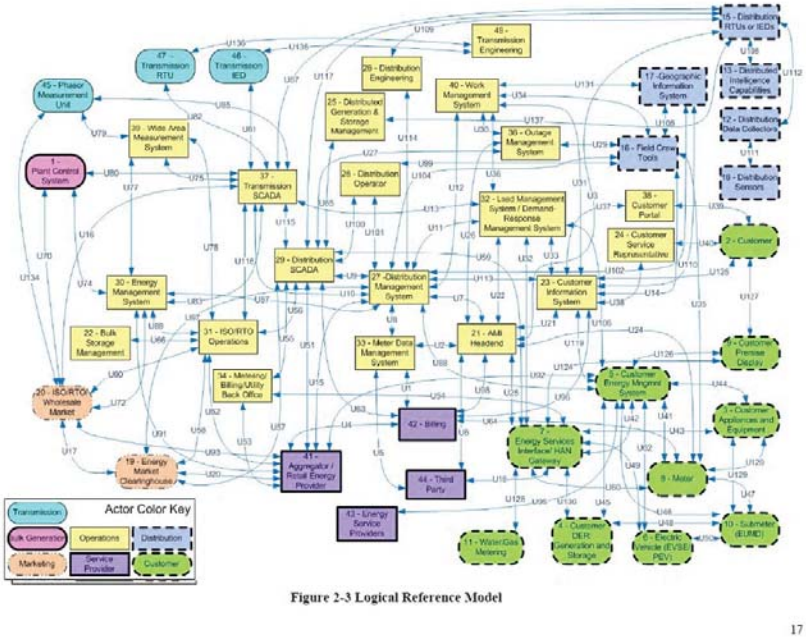

Fig. 3 Logical Reference Model [1]

interface categories that group logical interfaces based upon similar attributes affecting cyber security requirements; the logical interface categories are listed and described in Table 2-2. The grouping criteria include the three traditional Information Assurance dimensions: confidentiality, integrity, and availability. Other criteria include domain and logical interface information content. Each logical interface can be thought of as a layer in a three dimensional representation. As an example, Fig. 4 provides a graphical depiction of Logical

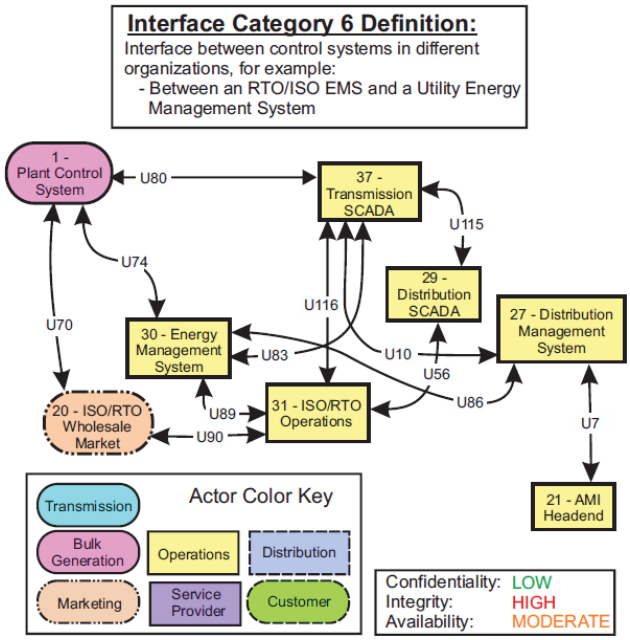

Fig. 5 Logical Interface Category 6, Interface between controls in different organizations [1]

Interface 6, which shows the interfaces between control systems (actors) in organizations in 3 domains.

In addition to the Logical Interface Categories defined in Chapter 2, NISTIR identifies 10 architecturally significant Use Cases that involve different actor and logical interface sets, which have similar complexity and graphical representations. These Use Cases include: advance metering architecture (AMI), Demand Response, Customer Interfaces, Electricity Market, Distribution Automation, Plug-in Hybrid Electric Vehicles (PHEV), Distributed Resources, Transmission Resources, Regional Transmission Operations / Independent System Operators (RTO/ISO), Operations, and Asset Management.

Over the course of 3 years of association with the TCIPG Project and studying NISTIR 7628, we have observed that the document was prepared by experts from three very disparate disciplines: power system engineers, computer and network engineers, and information technologist. There are relatively few experts in these disciplines with overlapping knowledge that bridges the gaps between these disciplines. Consequently, for most readers, the task of making sense of the very detailed and often unfamiliar information is quite daunting.

As a team, we have detailed knowledge of power systems but less knowledge of computer engineering and information management technologies. Therefore, our interest is developing a resource that dramatically accelerates the process of assembling data and information to facilitate synthesizing the complex ideas and relationships necessary to improve cyber security. We believe innovative approaches to visualizing NISTIR 7628's content would be a big step forward. Further, the user must be able define and adapt the

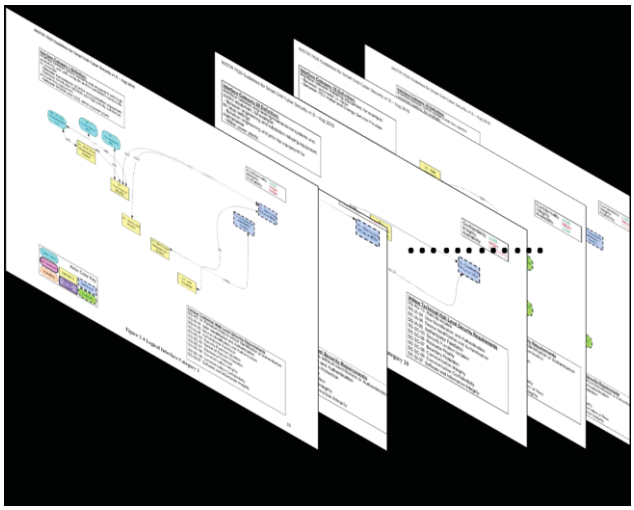

Fig. 4 Stacked Logical Interface Categories [1]

visualizations appropriate to his own knowledge base and purpose. We also envision the user being able to leverage other resources to seamlessly assemble other information appropriate to their purpose.

III. VISUALIZING NISTIR 7628

Our research vision is to create user controllable visual representations of the information in NISTIR 7628 to enable cyber security. The interactive interface would enable the user to organize information to provide insights that would otherwise be difficult to reach; this includes controlling the content and detail of information presented. For instance, we envision aiding the identification of common requirements across different Logical Interface Categories and Use Cases by displaying only that information. We also envision aiding the identification of common requirements across different Logical Interface Categories and Use Cases by displaying only that information. We also envision being able to pull-up and drill-into detailed information not a part of the current view – and open and close other related information as needed.

Our first small step to achieving this vision was to explore ways to stack select logical interface categories as distinct data layers. For example, consider the stacked Logical Interface Categories shown in Fig. 5 – an oblique visualization of several logical interface categories from pages taken directly from the document. This is helpful to illustrating the concept, but not very practical from productive use. We have developed two applications to explore implementing our ideas: 1) a web-based HTML application and 2) a MATLAB-based application leveraging 3D graphing capabilities.

A. HTML Web Page Visualization

The HTML-based visualization creates a data layer for each of the 22 logical interface categories; See Fig. 6. Users select the interface layers of interest on the list of 22 interface layers. The selected layers are displayed stacked from the straight-on perspective. The user sees the selected overlapping actors and their interfaces. The data layers can easily be toggled on and off with a mouse click making commonalities

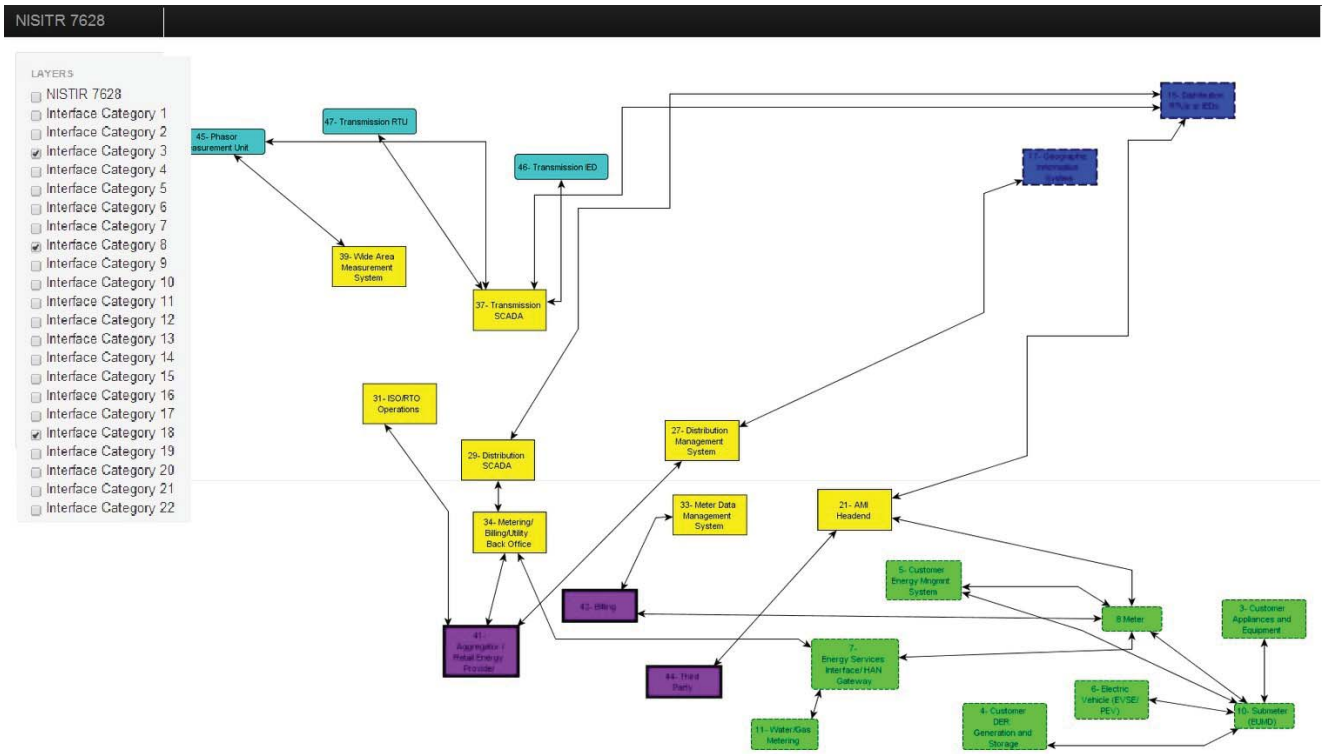

Fig. 6 HTML Model

and differences easy to identify. The web page's stacked depiction focuses the user's effort on the data without the tedium of thumbing through 50 pages in the document.

The web page visualization proved to be a good first step. However, from the outset, we know that it would sacrifice some information in the NISTIR's Logical Interface Category diagrams not easily captured with this approach. For example to see more detail about the interface between two actors, a user would still refer back to the paper document. The absence of the third dimension in the visualization made it difficult for the user to track which actors and interfaces were associated with each interface layer.

B. MATLAB Visualization

Our efforts to create the 3D representation using MATLAB were much more complex. The actors and interfaces for each logical interface category are assigned coordinates in the x-y plane. The logical interface categories are assigned coordinates on the z axis; see Fig. 3. Like the HTML model, interface categories of interest can be selected and stacked to focus upon the logical interface layers of interest. An attractive feature of the MATLAB representation is the graphical representation can be rotated in the three axes to gain the best view of the relationships of interest. The biggest feature this model has is the unique ability to rotate the model and visualize it from every angle.

Fig. 7 shows the top layer of the visualization model as represented in MATLAB, the actors portrayed are in the similar locations and color coded to the NISTIR 7628 layouts to minimize confusion as much as possible. The MATLAB tool allows a unique element to be added to model, which is a three dimensional layer that allows users to see the depth of the NISTIR 7628, something that has never been modeled before.

As well as the depth included in the MATLAB model, the information about each connection and relationship can be stored in the tool and accessed with a simple click of the button. This will allow people to understand and grasp a much larger amount of information with the simplicity of an application. Lacking in the MATLAB model is the clarity within a few aspects. Labeling the current model proved to be quite challenging. We found labels that work from a straight-on perspective can be quite difficult to read from other vantage points and create clutter that obscures important details.

We have presented the tool at several conference events with industry, government, and academic participants – and received very encouraging feedback.

C. NetAPT Visualization

NISTIR 7628 provided a conceptual construct for understanding the actors and their interaction. However, the NISTIR 7628 paradigm can provide misleading impressions about the physical implementations of the power grid's cyber systems. The Network Access Policy Tool (NetAPT) developed at the Information Trust Institute; University of Illinois at Urbana-Champaign provided a contracting graphical view of the actors and their interfaces. NetAPT ingests firewall rule information and uses it to generate a

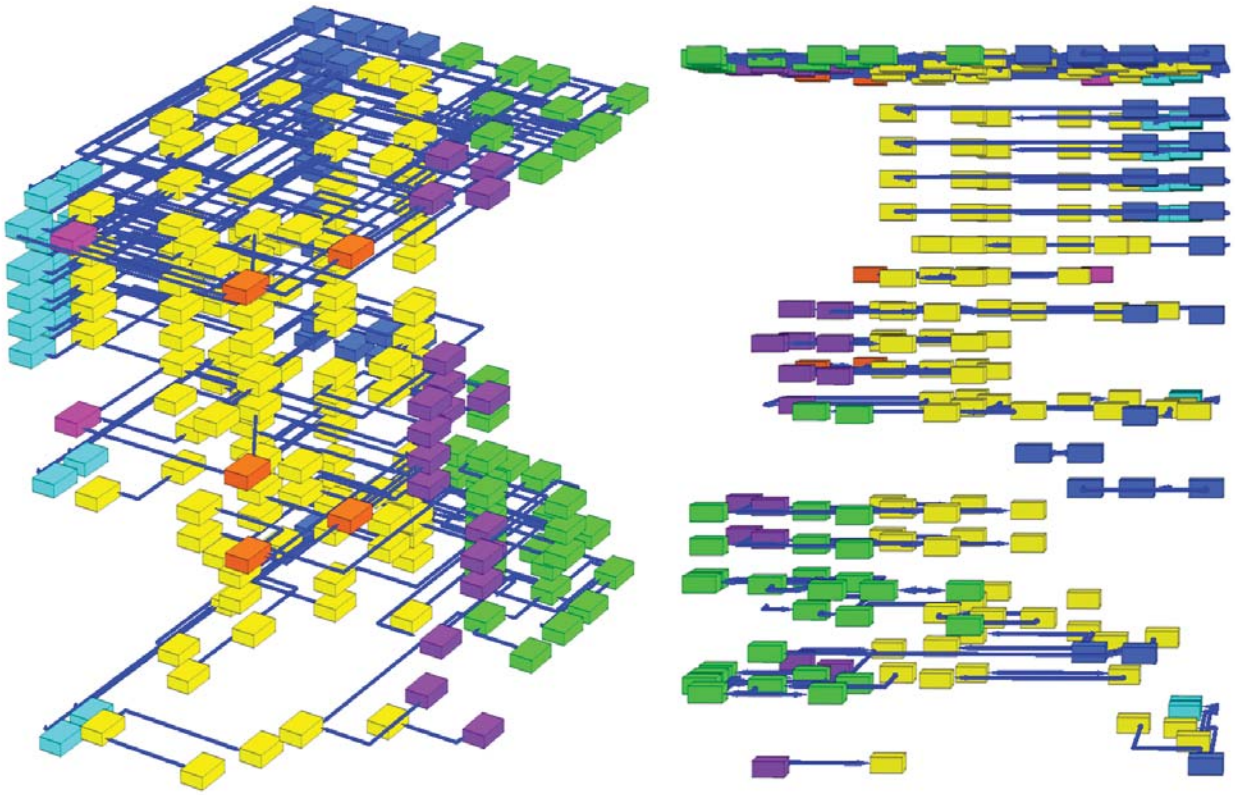

Fig. 7 MATLAB Model

graphical depiction – a depiction based upon actual system connections and less upon the conceptual functions captured in NISTIR 7628. Fig. 8 provided an example of a prototype power providers system. Now, this depiction has a much different structure than the NISTIR 7628 paradigm would produce. Both representations are valid. This poses interesting lines of investigation leveraging one representation against the other to gain insights that might otherwise not be apparent.

IV. Future Efforts

While our efforts to date have produced interesting and useful representations, we recognize that our progress is far from our envisioned functionality. Through our work to-date, we have gained an appreciation for the significant challenges involved.

In the near term, we are seeking off-the-shelf applications that can be adapted to our purposes. Immediate objectives include current and the following desired capabilities to

- Label graphical features and easily accommodate interactive perspective changes
- Easily zoom-in and pan-out
- Increase available information content, while affording the user robust displayed content control
- Automatically generate graphic layouts that are both useful and appealing form alternate perspectives
- Automatically ingest data to minimize the level of effort required to create, organize, and maintain the underlying "data stores"

A. Conclusions

With daily reports of attacks, there is an urgent need to broadly improve the power grids cyber security posture. The diversity and complexity of the measures environment. Consequently, it is very important that the efforts be placed against the most dangerous threat and vulnerability combinations. This drives the urgent need to understand the requirements established in documents like NISTIR 7628, which are extremely complex. We have demonstrated first steps to producing a graphical depiction that aids synthesizing key insights into the requirements. We have also refined our vision for an application to aid synthesizing complex cyber security information.

References

[1] NISTIR 7628: Guidelines to Smart Grid Cyber Security, NISTIR 7628, 2010.

[2] NetAPT Access Policy Tool. Web. Available: https://www.perform.illinois.edu/netapt/

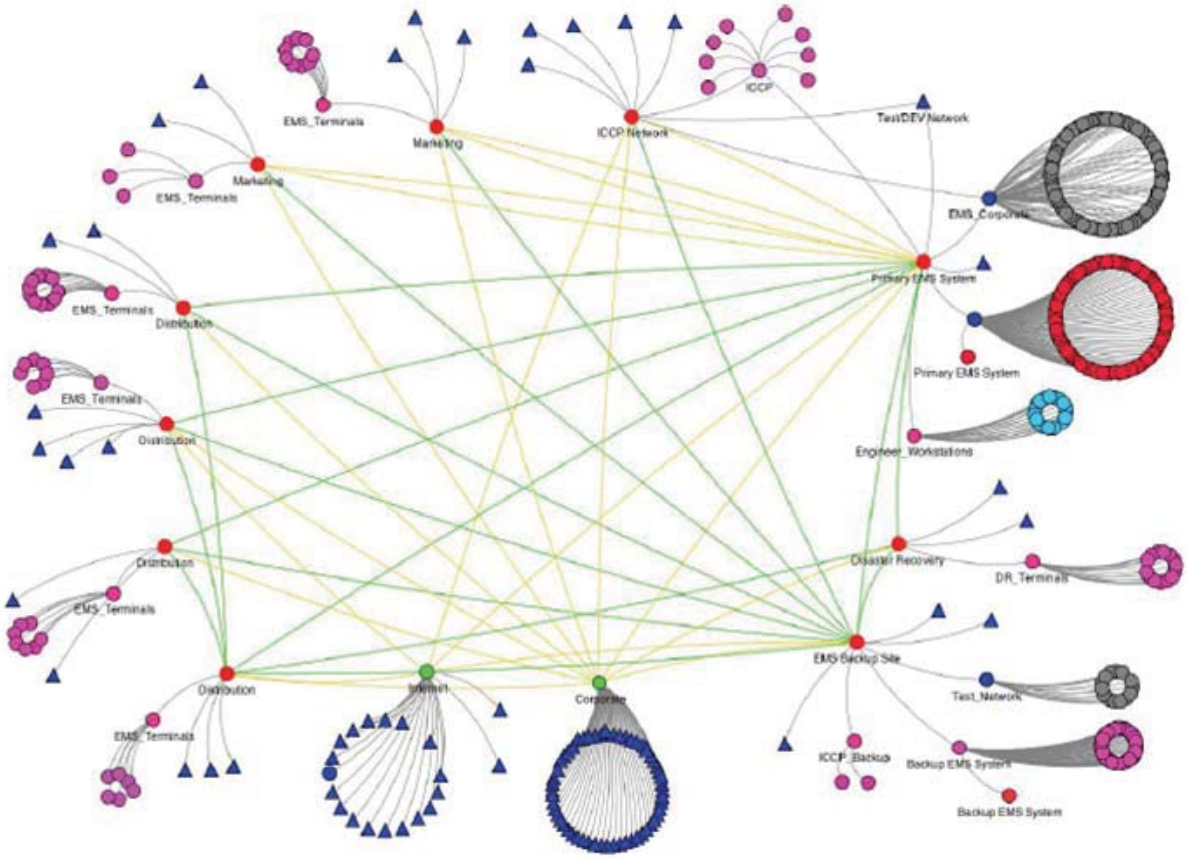

Fig. 8 TCIPG NetAPT Cyber Network Representation of Utility [2]

Table 2-2 Logical Interfaces by Category

Logical Interface Category	Logical Interfaces
1. Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints, for example: • Between transmission SCADA and substation equipment • Between distribution SCADA and high priority substation and pole-top equipment • Between SCADA and DCS within a power plant	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
2. Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints, for example: • Between distribution SCADA and lower priority pole-top equipment • Between pole-top IEDs and other pole-top IEDs	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
3. Interface between control systems and equipment with high availability, without compute nor bandwidth constraints, for example: • Between transmission SCADA and substation automation systems	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
4. Interface between control systems and equipment without high availability, without compute nor bandwidth constraints, for example: • Between distribution SCADA and backbone network-connected collector nodes for distribution pole-top IEDs	U3, U67, U79, U81, U82, U85, U102, U117, U135, U136, U137
5. Interface between control systems within the same organization, for example: • Multiple DMS systems belonging to the same utility • Between subsystems within DCS and ancillary control systems within a power plant	U9, U27, U65, U66, U89
6. Interface between control systems in different organizations, for example: • Between an RTO/ISO EMS and a utility energy management system	U7, U10, U13, U16, U56, U74, U80, U83, U87, U115, U116
7. Interface between back office systems under common management authority, for example: • Between a Customer Information System and a Meter Data Management System	U2, U22, U26, U31, U63, U96, U98, U110

Logical Interface Category	Logical Interfaces
8. Interface between back office systems not under common management authority, for example: • Between a third-party billing system and a utility meter data management system	U1, U6, U15, U55
9. Interface with B2B connections between systems usually involving financial or market transactions, for example: • Between a Retail aggregator and an Energy Clearinghouse	U4, U17, U20, U51, U52, U53, U57, U58, U70, U72, U90, U93, U97
10. Interface between control systems and non-control/corporate systems, for example: • Between a Work Management System and a Geographic Information System	U12, U30, U33, U36, U59, U75, U91, U106, U113, U114, U131
11. Interface between sensors and sensor networks for measuring environmental parameters, usually simple sensor devices with possibly analog measurements, for example: • Between a temperature sensor on a transformer and its receiver	U111
12. Interface between sensor networks and control systems, for example: • Between a sensor receiver and the substation master	U108, U112
13. Interface between systems that use the AMI network, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS	U8, U21, U25, U32, U95, U119, U130
14. Interface between systems that use the AMI network with high availability, for example: • Between MDMS and meters • Between LMS/DRMS and Customer EMS • Between DMS Applications and Customer DER • Between DMS Applications and DA Field Equipment	U8, U21, U25, U32, U95, U119, U130
15. Interface between systems that use customer (residential, commercial, and industrial) site networks which include: • Between Customer EMS and Customer Appliances • Between Customer EMS and Customer DER • Between Energy Service Interface and PEV	U42, U43, U44, U45, U49, U62, U120, U124, U126, U127

Logical Interface Category	Logical Interfaces
16. Interface between external systems and the customer site, for example: • Between Third Party and HAN Gateway • Between ESP and DER • Between Customer and CIS Web site	U18, U37, U38, U39, U40, U88, U92, U100, U101, U125
17. Interface between systems and mobile field crew laptops/equipment, for example: • Between field crews and GIS • Between field crews and substation equipment	U14, U29, U34, U35, U99, U104, U105
18. Interface between metering equipment, for example: • Between sub-meter to meter • Between PEV meter and Energy Service Provider	U24, U41, U46, U47, U48, U50, U54, U60, U64, U128, U129
19. Interface between operations decision support systems, for example: • Between WAMS and ISO/RTO	U77, U78, U134
20. Interface between engineering/maintenance systems and control equipment, for example: • Between engineering and substation relaying equipment for relay settings • Between engineering and pole-top equipment for maintenance • Within power plants	U11, U109
21. Interface between control systems and their vendors for standard maintenance and service, for example: • Between SCADA system and its vendor	U5
22. Interface between security/network/system management consoles and all networks and systems, for example: • Between a security console and network routers, firewalls, computer systems, and network nodes	U133 (includes interfaces to actors 17-Geographic Information System, 12 – Distribution Data Collector, 38 – Customer Portal, 24 – Customer Service Representative, 23 – Customer Information System, 21 – AMI Headend, 42 – Billing, 44 – Third Party, 43 – Energy Service Provider, 41 – Aggregator / Retail Energy Provider, 19 – Energy Market Clearinghouse, 34 – Metering / Billing / Utility Back Office)

2.3.1 Logical Interface Categories 1—4

Logical Interface Category 1: Interface between control systems and equipment with high availability, and with compute and/or bandwidth constraints

Logical Interface Category 2: Interface between control systems and equipment without high availability, but with compute and/or bandwidth constraints

Logical Interface Category 3: Interface between control systems and equipment with high availability, without compute or bandwidth constraints

Logical Interface Category 4: Interface between control systems and equipment without high availability, without compute or bandwidth constraints

Logical interface categories 1 through 4 cover communications between control systems (typically centralized applications such as a SCADA master station) and equipment as well as communications between equipment. The equipment is categorized with or without high availability. The interface communication channel is categorized with or without computational and/or bandwidth constraints. All activities involved with logical interface categories 1 through 4 are typically machine-to-machine actions. Furthermore, communication modes and types are similar between logical interface categories 1 through 4 and are defined as follows:

- Interface Data Communication Mode
  - Near Real-Time Frequency Monitoring Mode (ms, subcycle based on a 60 Hz system) (may or may not include control action communication)
  - High Frequency Monitoring Mode (2 s ≤ 60 s scan rates)
  - Low Frequency Monitoring Mode (scan/update rates in excess of 1 min, file transfers)
- Interface Data Communication Type
  - Monitoring and Control Data for real-time control system environment (typical measurement and control points)
  - Equipment Maintenance and Analysis (numerous measurements on field equipment that is typically used for preventive maintenance and post analysis)
  - Equipment Management Channel (remote maintenance of equipment)

The characteristics that vary between and distinguish each logical interface category are the availability requirements for the interface and the computational/communications constraints for the interface as follows:

- Availability Requirements – Availability requirements will vary between these interfaces and are driven primarily by the power system application which the interface supports and not by the interface itself. For example, a SCADA interface to a substation or pole-top RTU may have a HIGH availability requirement in one case because it is supporting critical monitoring and switching functions or a MODERATE to LOW availability if supporting an asset-monitoring application.