Analytics for Enterprise Cybersecurity

Management of Smart Grid Cyber Risks & Vulnerabilities

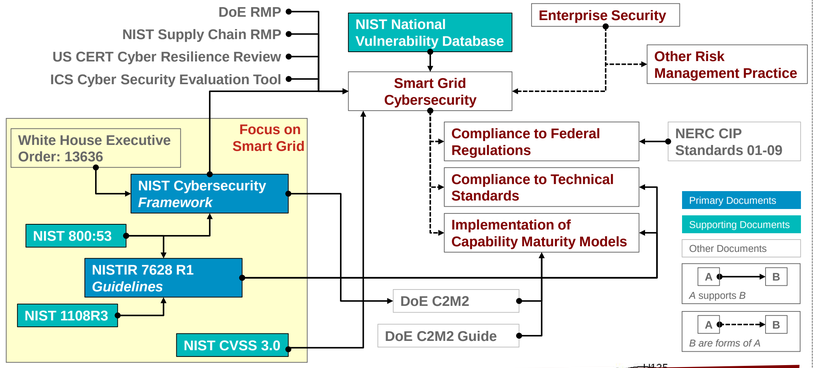
Nazli Choucri
Professor of Political Science
nchoucri@mit.edu

Gaurav Agarwal
Research Affiliate, MIT Political Science
gauravag@mit.edu

Integrated Smart Grid Cybersecurity Approach

The challenge is to retrieve and examine the knowledge embedded in the text and, as needed, capture its utility.

- Difficult to aggregate and integrate across guidelines in text form.
- Text impedes locating interactions, feedback, specialized views, etc.
- Undermine the full value effectiveness of guidelines and directives.



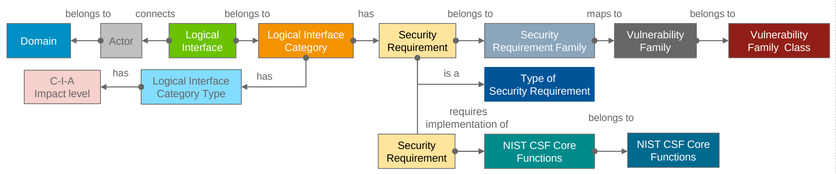
Solution Strategy: Deploy Analytical Methods to Capture Full Value of Cybersecurity Guidelines.

Steps for Analyzing Smart Grid Cybersecurity

A	**Create Linked Data for Smart Grid Reference Model**	Identify essential system elements designed to fulfil intended functions of a Smart Grid and create a linked database.	***Sources:*** NIST: 7628 - Guidelines for Smart Grid Cybersecurity; NIST Cybersecurity Framework ***Tools:*** *Relational Database tools.*
B	**Construct Design Structure Matrix & Exploratory Tools**	Construct Design Structure Matrix (DSM) based on essential elements of Smart Grid and its Cybersecurity.	***Source:*** Relational Database created in Step 1. ***Tools:*** *Excel for DSMs; Tableau for exploratory tool; Protégé for Hypertext views.*
C	**Construct Network View**	Create network view from reference model to examine dependencies among system elements, to examine implications of guidelines for Smart Grid and Cybersecurity.	***Source:*** Relational Database created in Step A. ***Tools:*** *Gephi for creating network visualizations.*
D	**Focus on Risk Identification and Assessment**	Utilize exploratory tools, databases and network views to situate vulnerabilities of system elements and analyse system-wide impacts on the smart grid using network views.	***Additional Sources:*** NIST National Vulnerability Database; NIST CVSS ***Tools:*** *DSMs (Excel); Exploratory Tools (Tableau) ; Hypertext (Protégé) and Network visualizations (Gephi)*

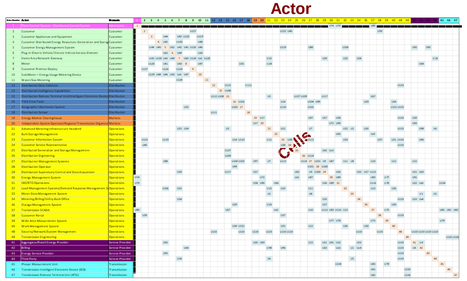
A. Linked Data for Smart Grid Reference Model

Linked database of information available in select policy documents.



B. Design Structure Matrix of Smart Grid Reference Model

Extract data and information on Smart Grid Domain elements from NIST: 7628 Guidelines for Smart Grid Cybersecurity



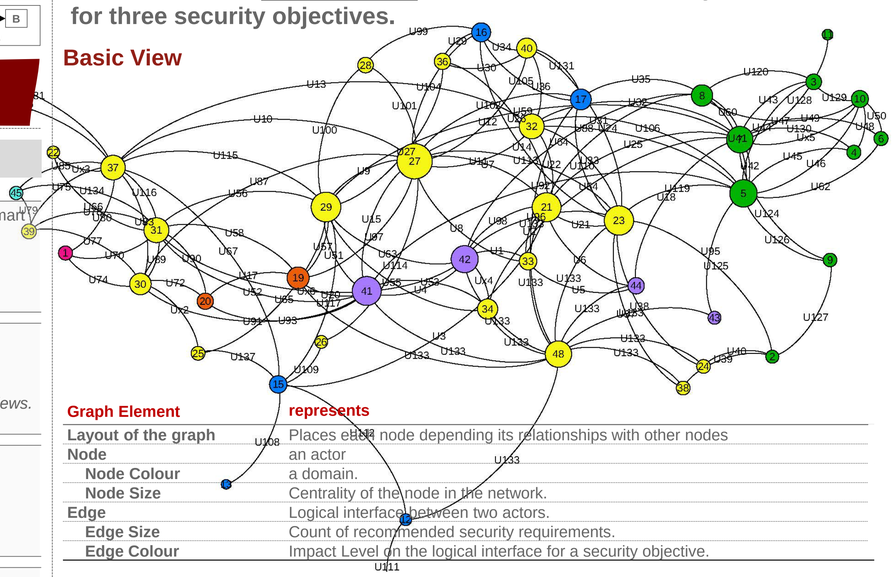
Cells contain the following information based on four set of information provided in NISTIR- 7628 on:

- **Logical Interface** between any two actors
- **Logical Interface Categories** based on Interface attributes.
- **Impact Level** of Logical Interface for three Security Objectives.
- Count of **Security Requirements** applicable for each Logical Interface.

C. Network View for Impact Evaluation

Identification of impact levels on interfaces between any two actors for three security objectives.

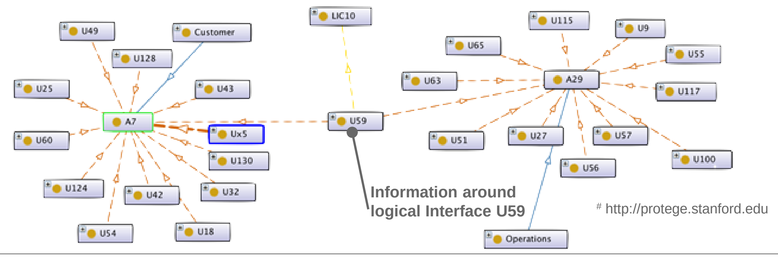
Basic View



Graph Element	represents
Layout of the graph	Places each node depending its relationships with other nodes
Node	an actor
Node Colour	a domain.
Node Size	Centrality of the node in the network.
Edge	Logical interface between two actors.
Edge Size	Count of recommended security requirements.
Edge Colour	Impact Level on the logical interface for a security objective.

C. Exploratory Tools for Vulnerability Identification

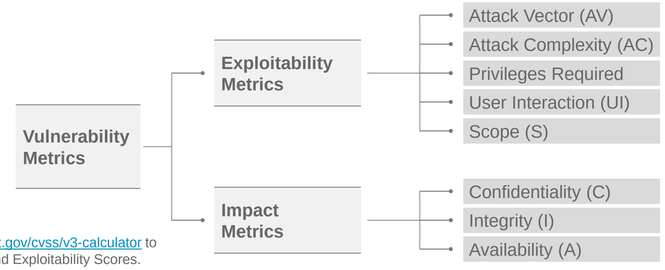
Transform Linked Data into hypertext form using Protégé# for risk/vulnerability identification



http://protege.stanford.edu

D-1. Metrics for Risk Quantification

Identify risk exploitability and impact attributes as defined in NIST CVSS 3.0



Visit https://nvd.nist.gov/cvss/v3-calculator to calculate Impact and Exploitability Scores.

D-2. Quantification of a Cyber Vulnerability

Numerical score reflecting severity (Impact) and exploitability of a risk based on Cyber Vulnerability Scoring System (CVSS 3.0)

$$Exploitability\ Score = 8.22 \times AV \times AC \times PR \times UI$$

$$Impact\ Score(Scope\ Unchanged) = 6.42 \times ISC_{Base}$$

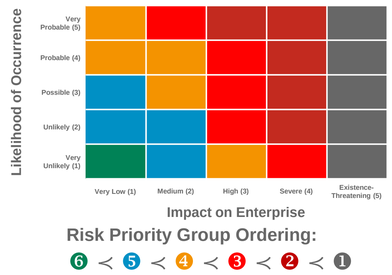
$$Impact\ Score(Scope\ Changed) = 7.52 \times (ISC_{Base} - 0.029) + 3.25 \times (ISC_{Base} - 0.02)^{15}$$

where,

$$ISC_{Base} = 1 - (1 - C) \times (1 - I) \times (1 - A)$$

D-3. Transformation of Risk to Enterprise Relevance

Transform CVSS Metrics into enterprise objectives and locate individual risks on the Risk Matrix.



Risk Priority Group Ordering:

6 ≺ 5 ≺ 4 ≺ 3 ≺ 2 ≺ 1

Likelihood of Occurrence

Determine likelihood, based on:

- Historic data
- Internal Assessments for realistic case/ scenario
- Engineering Risk Benefit Analysis

$$Likelihood = f(CVSS\ Exploitability\ Score)$$

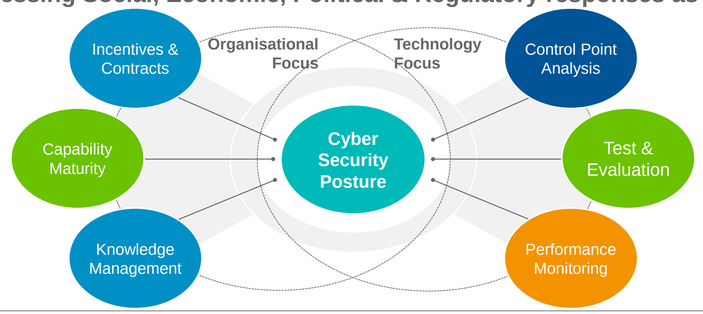
Impact on Enterprise

- Compromised National Security
- Loss of business or loss of Sales/ EBIT
- Clean-up and recovery costs

$$Impact = f(CVSS\ Imapct\ Score)$$

D-4. Strategies for Risk Mitigation

Systematic analysis of Scientific & Technical solutions, and addressing Social, Economic, Political & Regulatory responses as well.



Massachusetts Institute of Technology

- Analytics for Cyber-Physical System Cybersecurity: Policy-Governed Secure Collaboration
- See https://cps-vo.org/VU_AnalyticsforCPS-Cybersecurity for details.

September 01, 2022