DEVELOPING RISK METHODOLOGY WITHIN U.S. SMART GRID SYSTEM

Saatvik Mohan, Vanderbilt University
Mentor: Dr. Mathias Uslar, OFFIS

Introduction

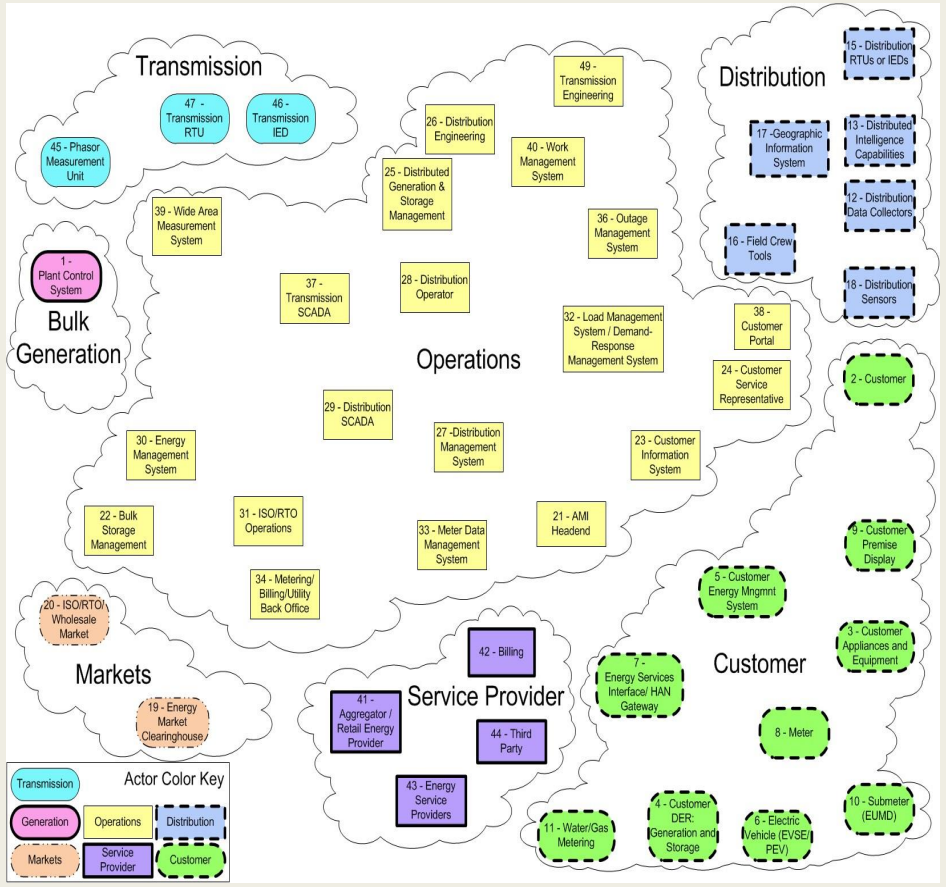
- NIST: *Guidelines for Smart Grid Cybersecurity*
- Evolution of cybersecurity
- Contribution of *Guidelines*
  - Actor descriptions
  - Composite view of actors within domains
  - Logical reference model
  - CIA levels for LICs
  - Mitigations for LICs
- Limitations
  - No way to define criticality of actors
  - Inconsistencies
  - No methodology to define risk of system or category of systems

Background Terminology

- Actor/System
- Domain
- Zone
- Logical Interface (Category)
- Risk Formula
  - Function of threat, vulnerability, and consequence (impact)
    - Interagency Security Committee: *The Risk Management Process for Federal Facilities*

Goal

- Develop methodology and risk formulas that all players in the smart grid can utilize
- Subjective decisions, but analysis itself is based primarily on quantitative data
- Two formulas
  - 1: Actors defined in the Logical Inference Model
  - 2: 8 categories that were created from the 22 LICs



Actors in Domains
Source: *Guidelines*

Formula 2 Categories

- make overarching categories from the 22 LICs
- easier to identify certain general descriptions/characteristics that can be given a risk value
- similarities taken into account:
  - Types of domains actors found in
  - Shared actors
  - Functions
- Not mutual exclusive or disparate

Description	LICs
Interface between control systems and equipment	1,2,3,4
Critical information exchange between utility and third party	6,9,19
Non-critical information exchange between utility and third party	7,8,17,21
Metering & billing	10,13,14,16,18
Distrbution domain	11,12
Controlled system to back-end system	5,8,20
Customer domain	15
Interface between security/network/system management consoles and all networks and systems	22

Formula 2 Categories

Threat

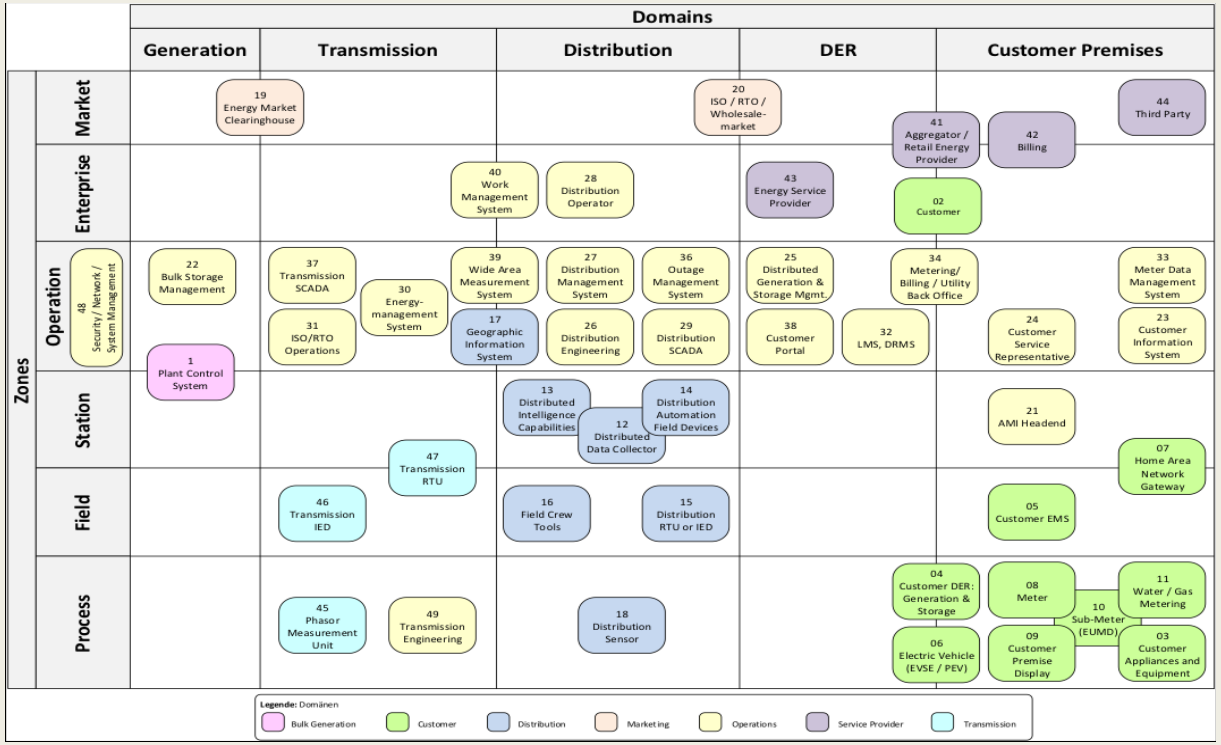
- *Guidelines* provides no quantifiable threat levels
- Smart Grid Architecture Model (SGAM)
  - provides threat values based on where different domains and zones intersect

SGIS-SL HIGH LEVEL GUIDANCE*						
3 – 4	3 – 4	3 – 4	2 – 3	2 – 3	MARKET	ZONES
3 – 4	3 – 4	3 – 4	2 – 3	2 – 3	ENTREPRISE	
3 – 4	5	3 -4	3	2 – 3	OPERATION	
2 – 3	4	2	1 – 2	2	STATION	
2 – 3	3	2	1 – 2	1	FIELD	
2 - 3	2	2	1 - 2	1	PROCESSES	
GENERATION	TRANSMISSION	DISTRIBUTION	DER	CUSTOMER		
DOMAINS						

Threat Value Recommendation Per Layer
Source: *Smart Grid Information Security*

Security Level	Security Level Name	Europeans Grid Stability Scenario Security Level Examples
5	Highly Critical	Assets whose disruption could lead to a power loss above 10 GW Pan European Incident
4	Critical	Assets whose disruption could lead to a power loss from above 1 GW to 10 GW European / Country Incident
3	High	Assets whose disruption could lead to a power loss from above 100 MW to 1 GW Country / Regional Incident
2	Medium	Assets whose disruption could lead to a power loss from 1 MW to 100 MW Regional / Town Incident
1	Low	Assets whose disruption could lead to a power loss under 1 MW Town / Neighborhood Incident

Threat Value Descriptions
Source: *Smart Grid Information Security*



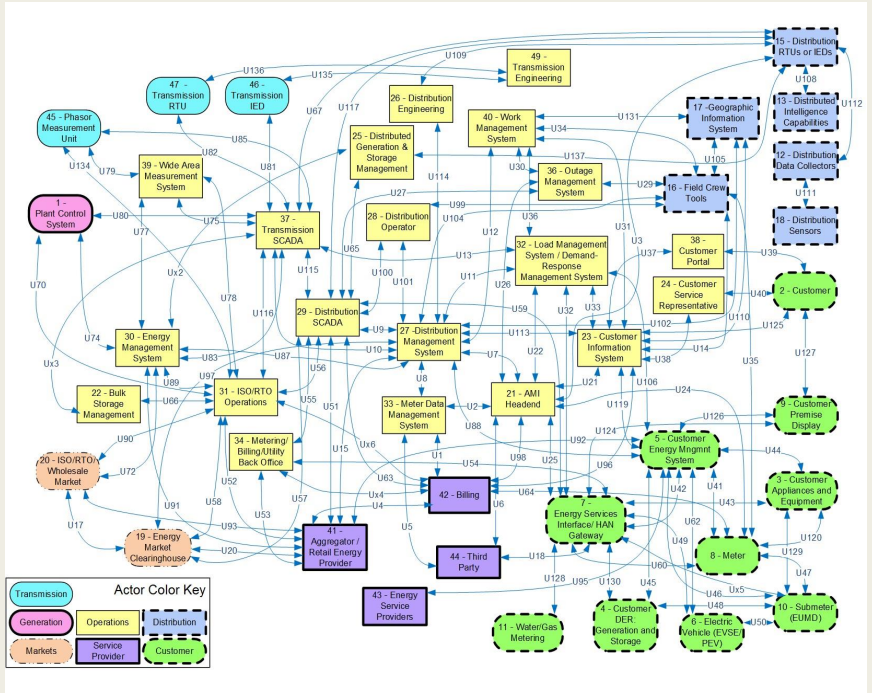
Actors Mapped onto SGAM

Threat Components

- Formula 1
  - 1. Threat value of each actor
  - 2. Average threat value of all bordering actors
- Formula 2
  - 1. Average threat value of actors
    - calculated by dividing the sum of all threat values of all actors by the number of appearances of those actors

Vulnerability

- Actors are interdependent because of interfaces that connect them
- Quantifying vulnerability is important because a system becoming compromised can leave many others vulnerable
- Inconsistency



Logical Interfaces Between Actors
Source: *Guidelines*

Vulnerability Components

- Formula 1
  - 1. Number of logical interfaces
  - 2. Number of domains spanned by interfaces
    - More domains an attacker gains access to, more vulnerable entire smart grid becomes
- Formula 2
  - 1. Number of domains that the LICs collectively spanned
  - 2. Average number of actors found in LICs

Impact

- Takes into account just how devastating an attack on a particular actor of type of actor is
- CIA
- Other security characteristics

Table 4 – Impact Level Descriptions
Source: *Guidelines*

	Potential Impact Levels		
	Low	**Moderate**	**High**
Confidentiality Preserving authorized restrictions on information access and disclosure, including means for protecting personal privacy and proprietary information.	The unauthorized disclosure of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized disclosure of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Integrity Guarding against improper information modification or destruction, and includes ensuring information non-repudiation and authenticity.	The unauthorized modification or destruction of information could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The unauthorized modification or destruction of information could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.
Availability Ensuring timely and reliable access to and use of information.	The disruption of access to or use of information or an information system could be expected to have a **limited** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **serious** adverse effect on organizational operations, organizational assets, or individuals.	The disruption of access to or use of information or an information system could be expected to have a **severe or catastrophic** adverse effect on organizational operations, organizational assets, or individuals.

Logical Interface Category	Confidentiality	Integrity	Availability
1	L	H	H
2	L	H	M
3	L	H	H
4	L	H	M
5	L	H	H
6	L	H	M
7	H	H	L
8	H	H	L
9	H	H	M
10	L	H	M
11	L	M	M
12	L	M	M
13	H	H	L
14	H	H	H
15	L	M	M
16	H	M	L
17	L	H	M
18	M	H	L
19	L	H	M
20	L	H	M
21	L	H	M
22	H	H	H

CIA Impact Levels
Source: *Guidelines*

Impact Components

- Formula 1 & 2
  - 1. Confidentiality Score
  - 2. Impact Score
  - 3. Availability Score
- Formula 1: logical interfaces of each actor belong to certain LIC
  - Each actor's logical interfaces have impact levels for three components
  - Values were averaged across these interfaces to find CIA scores
- Formula 2: LICs in all 8 categories were averaged for their CIA scores

What makes a Good Formula

- Accuracy
  - Correct weightings and offset, function
- Normality
  - Kurtosis (tail-heaviness) and skewness (measure of symmetry) close to 0
- Usability
  - Scale down values using $f(x) = \frac{(b-a)*(x-\text{min.})}{max.-min.} + a$

Conclusion

- Formula 1:
  - Risk = (Threat Value*Threat of Bordering Actors)+((Number of Logical Interfaces/3)*Number of Domains)+(0.25 * (C Score+0.5)*(I Score+1)*(A Score+2))
  - Kurtosis: -0.187, skewness: 0.598
- Formula 2:
  - Risk = 2.25*Threat Value + (0.7)*(Number of domains+(Average Number of Actors/2)) + (0.125*(C Score+0.5)*(I Score+1)*(A Score+2))
  - Kurtosis: -0.132, skewness: -0.749

	Actor	Formula 1 (Scaled)
1	Plant Control System	5.68
2	Customer	3.28
3	Customer Appliances and Equipment	1.09
4	Customer DER: Generation & Storage	2.12
5	Customer EMS	4.20
6	Electric Vehicle(EVSE/PEV)	1.40
7	Home Area Network Gateway	4.85
8	Meter	3.53
9	Customer Premise Display	1.00
10	Sub-Meter	1.80
11	Water/Gas Metering	1.53
12	Distributed Data Collector	1.38
13	Distributed Intelligence Capabilities	1.30
15	Distribution RTU or IED	3.12
16	Field Crew Tools	3.56
17	Geographic Information System	5.38
18	Distribution Sensor	1.30
19	Energy Market Clearinghouse	7.28
20	ISO/RTO/Wholesale-market	7.06
21	AMI Headend	6.31
22	Bulk Storage Management	5.38
23	Customer Information System	6.85
24	Customer Service Representative	3.45
25	Distributed Generation & Storage Mgmt.	3.84
26	Distribution Engineering	3.70
27	Distribution Management System	10.00
28	Distribution Operator	4.16
29	Distribution SCADA	9.09
30	Energy-Management System	8.13
31	ISO/RTO Operations	9.64
32	LMS, DRMS	4.37
33	Meter Data Management System	4.35
34	Metering/Billing/Utility Back Office	4.92
36	Outage Management System	4.47
37	Transmission SCADA	8.72
38	Customer Portal	3.45
39	Wide Area Measurement System	6.17
40	Work Management System	5.01
41	Aggregator/Retail Energy Provider	6.96
42	Billing	5.66
43	Energy Service Provider	2.78
44	Third Party	3.32
45	Phasor Measurement Unit	3.57
46	Transmission IED	3.45
47	Transmission RTU	4.25
49	Transmission Engineering	2.56

Formula 1 - Scaled Risk Value

	Description	Formula 2 (Scaled)
1	Interface between control systems and equipment	6.6
2	Critical information exchange between utility and third party	7.7
3	Non-critical information exchange between utility and third party	6.3
4	Metering & billing	7.0
5	Distrbution domain	1.0
6	Controlled system to back-end system	6.7
7	Customer domain	1.7
8	Interface between security/network/system management consoles and all networks and systems	10.0

Formula 2 - Scaled Risk Value

Use Case: Puerto Rican Smart Meter

- 2009: Puerto Rican smart meters hacked by attackers using optical converter device that allowed them to alter the settings for recording power consumption.
  - Speculative estimate of $400 million annually
  - difficult to quantify the adverse effects resulting after a system like this one has been compromised.

	Actor	Threat	Threat of Bordering Actors	Number of Logical Interfaces	Number of Domains	Confidentiality Score	Integrity Score	Availability Score	Formula 1 (Unscaled)	Formula 1 (Scaled)
8	Meter	1	1.71	7	4	1.78	2.83	1.44	18.57	3.53

	Description	Threat Value	Number of Domains	Average Number of Actors	Confidentiality Score	Integrity Score	Availability Score	Formula 2 (Unscaled)	Formula 2 (Scaled)
4	Metering & billing	2.73	4.00	11.20	2.40	2.80	1.60	17.83	7.0

Discussion

- Limitations
  - Subjective decisions for values included
    - Other security characteristics: authenticity, attack signature, computing power, latency, professionalism of attacker
  - Formula 2's categories
- Future Work
  - Changing formula
  - Inclusion of mitigations: common and unique
  - TLP

Sources

- *Guidelines for Smart Grid Cybersecurity,* NIST
- *Smart Grid Information Security,* Smart Grid Coordination Group
- https://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/
- *The Risk Management Process for Federal Facilities,* Interagency Security Committee