
Human motivation and the
security of IoT - Smart Grid
Adam Szekeres
NTNU i Gjøvik
9.06.2016

Overview

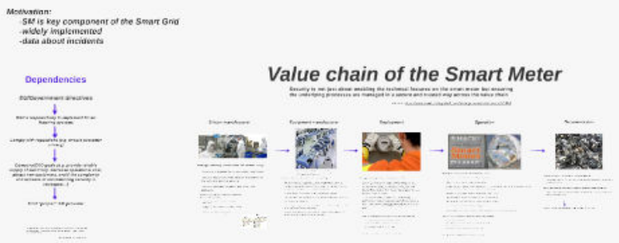
Conflicting Incentives Risk Analysis (CIRA)

Novel risk analysis method

- Concepts from Game Theory, Behavioral Economics, Decision Making, Psychology
- Replace probability estimates by stakeholder incentives and motivation
- Focus on **Human factors** - motivation
- **Risk is subjective**
- Conscious, **strategic behavior**, trade-off decisions
- Two types of risk: **threat risk & opportunity risk**
- Search for **negative externalities** or **moral hazards**

Approaching the Smart Grid

Case study for demonstration - Threats during the Smart Meter's life cycle



Conflicting Incentives Risk Analysis (CIRA)

Novel risk analysis method

Concepts from Game Theory, Behavioral Economics, Decision Making, Psychology

Replace probability estimates by stakeholder incentives and motivation

Focus on **Human factors** - motivation

Risk is subjective

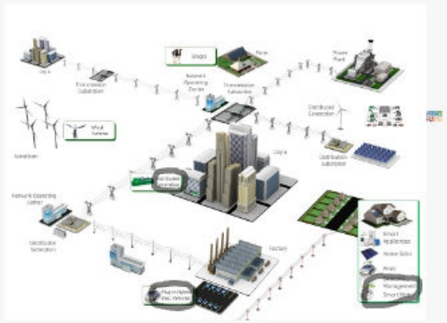
Conscious, **strategic behavior**, trade-off decisions

Two types of risk: **threat risk & opportunity risk**

Search for **negative externalities** or **moral hazards**

Approaching the Smart Grid

High-level overview of the Smart Grid



4. Identify key CIRA concepts:

Based on a specific requirement -> Define scope/ boundaries

Identify stakeholders:
-risk owner
-strategy owner(s)

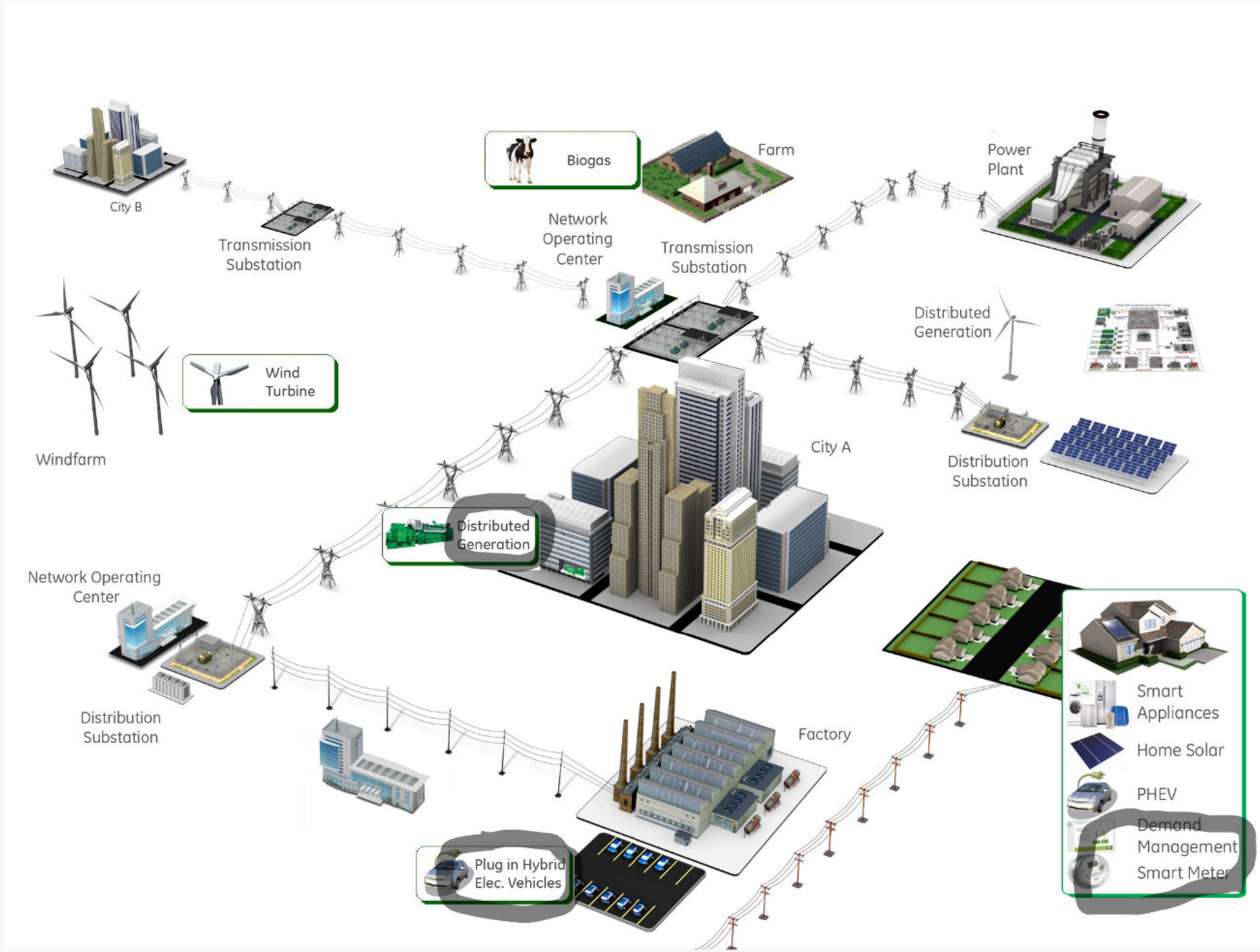
Identify strategies (actions to increase perceived utility, modify risk owner's utility)

Identify utilities for each stakeholder:
-utility factors (e.g. wealth, reputation...)

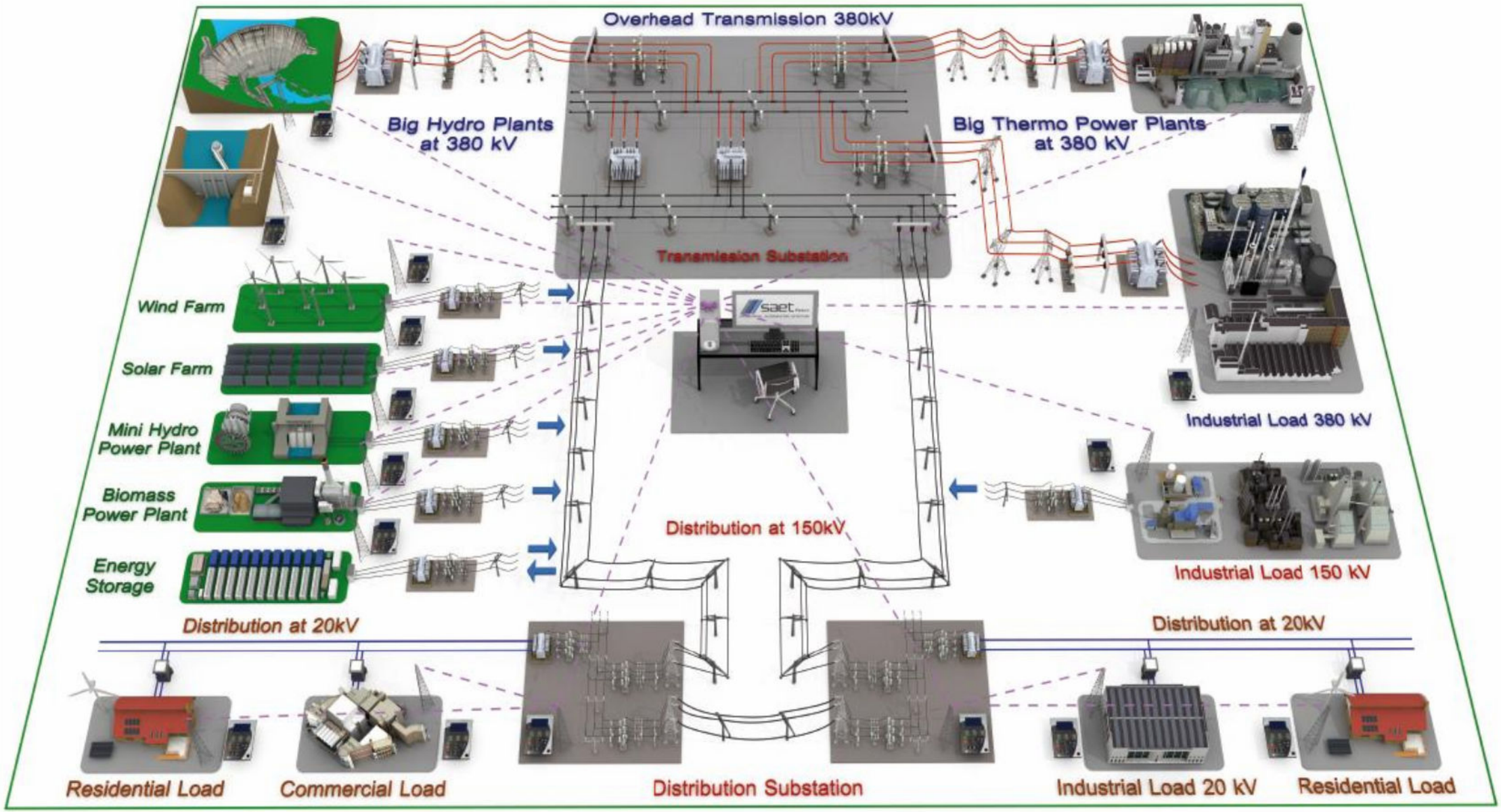
5. Identify actual persons based on roles and associated responsibilities within a company

6. Check whether stakeholder utilities are misaligned
Threat Risk - Opportunity Risk

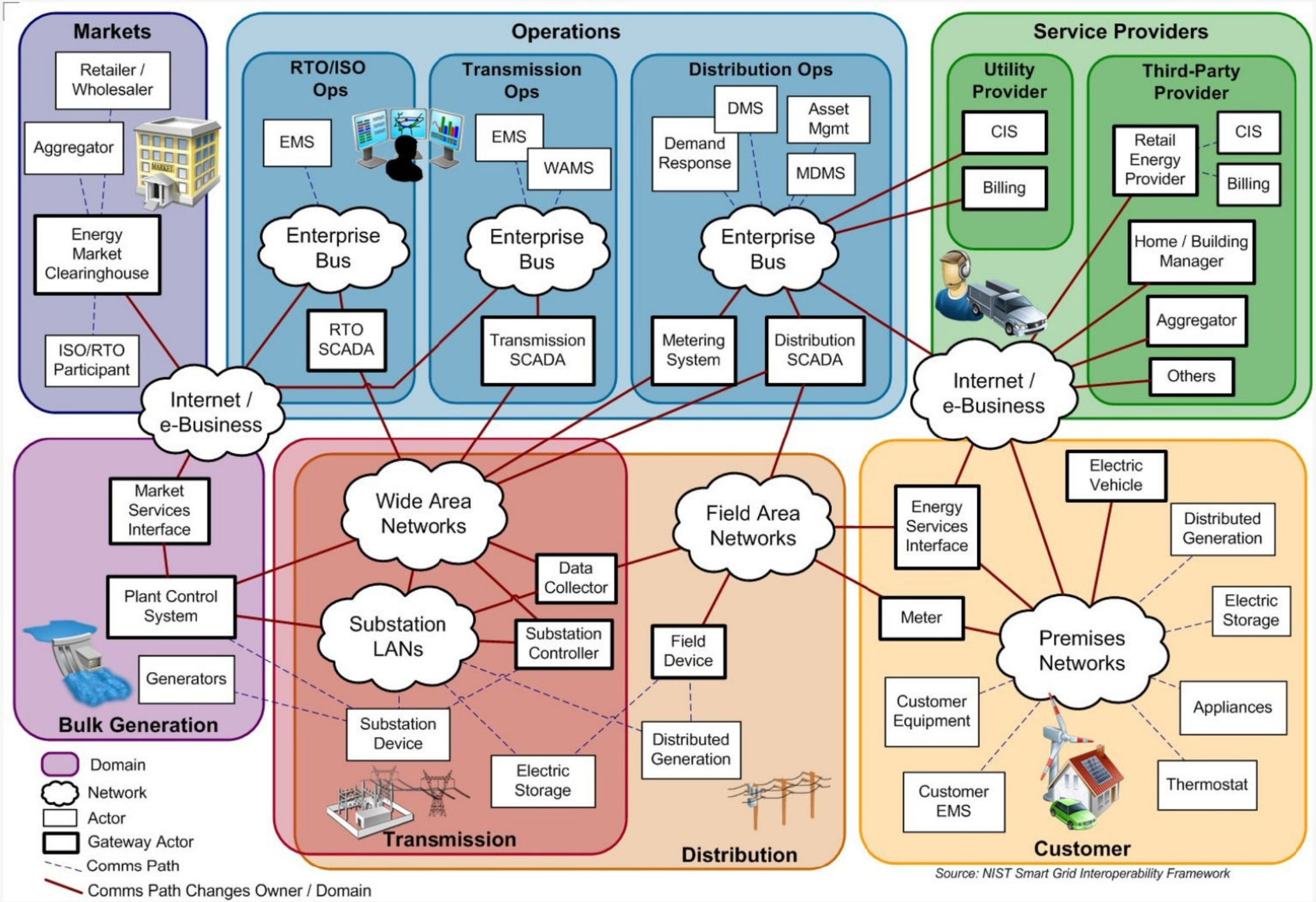
High-level overview of the Smart Grid



2-way flow of electricity and information

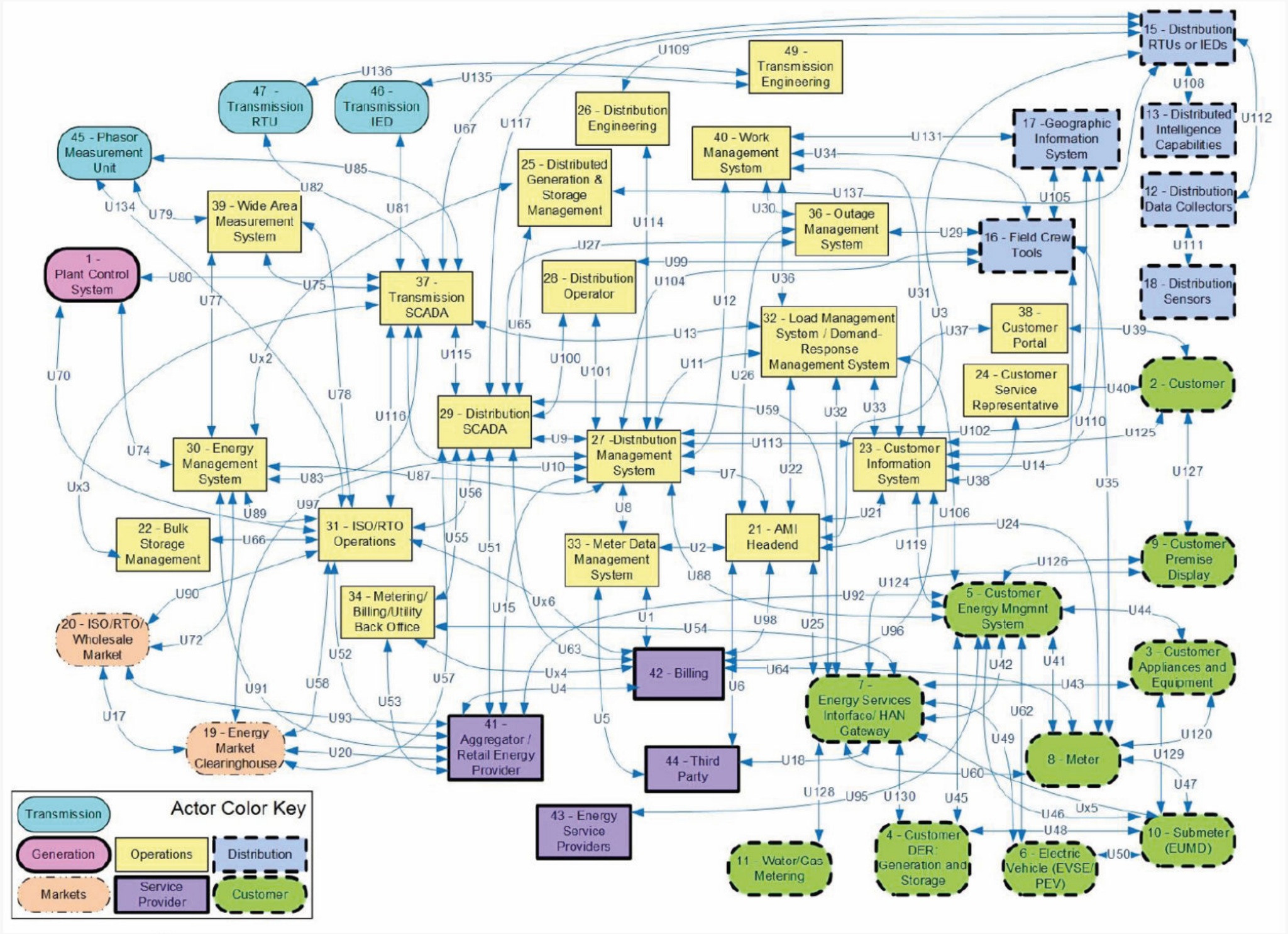


Smart Grid domains with communication channels



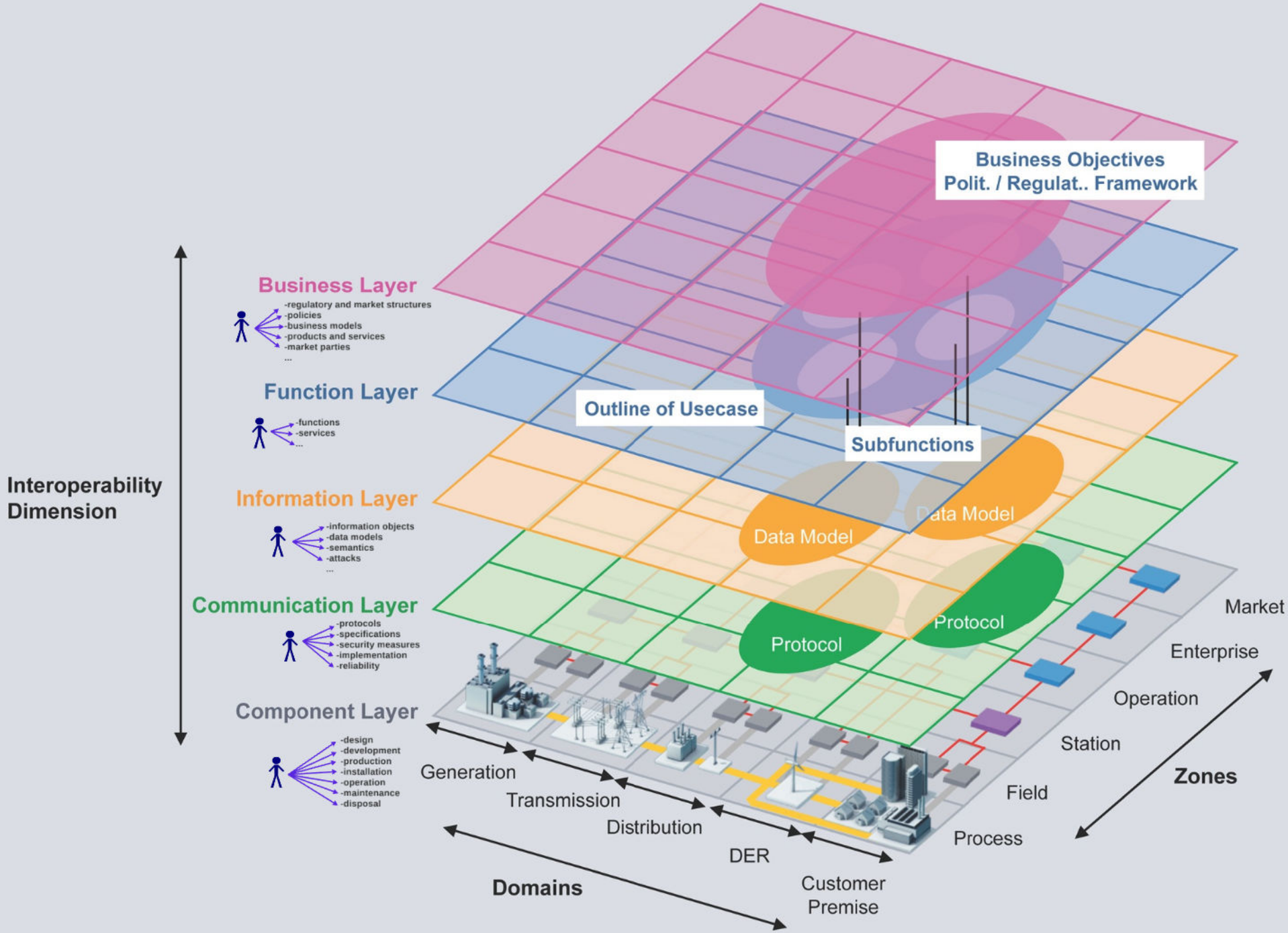
Source: NIST Smart Grid Interoperability Framework

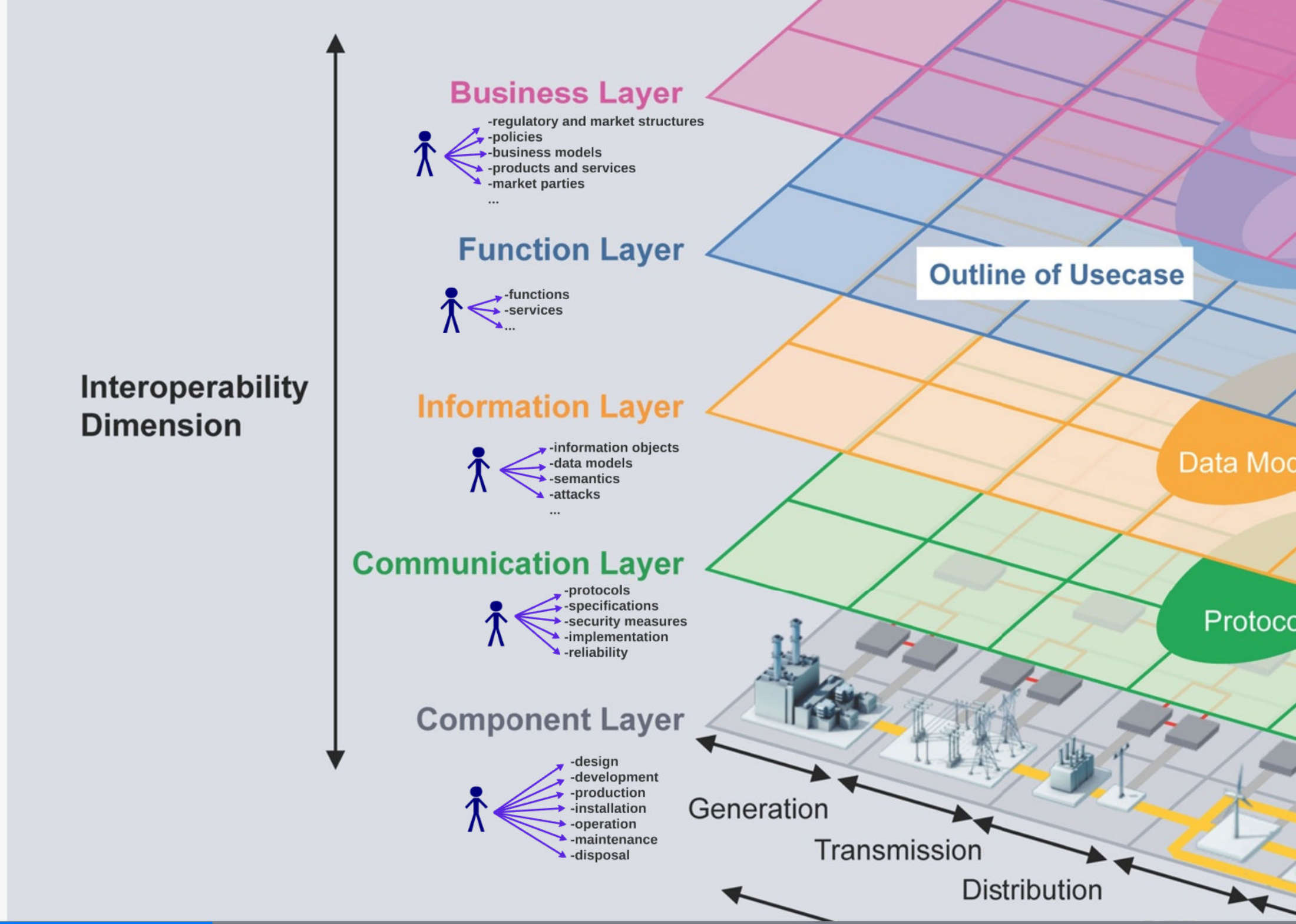
Components and their interactions

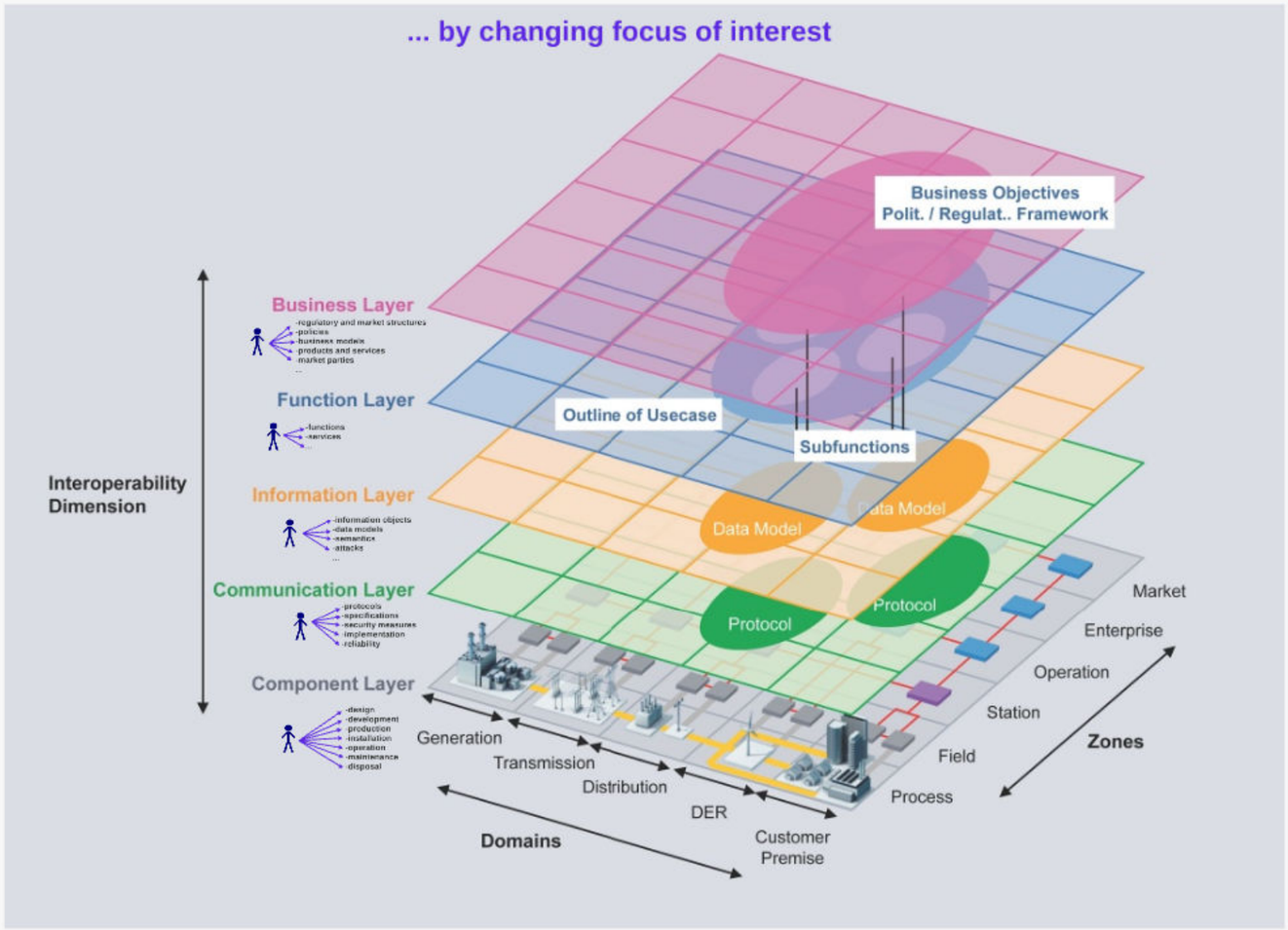


How to handle the complexity?

... by changing focus of interest

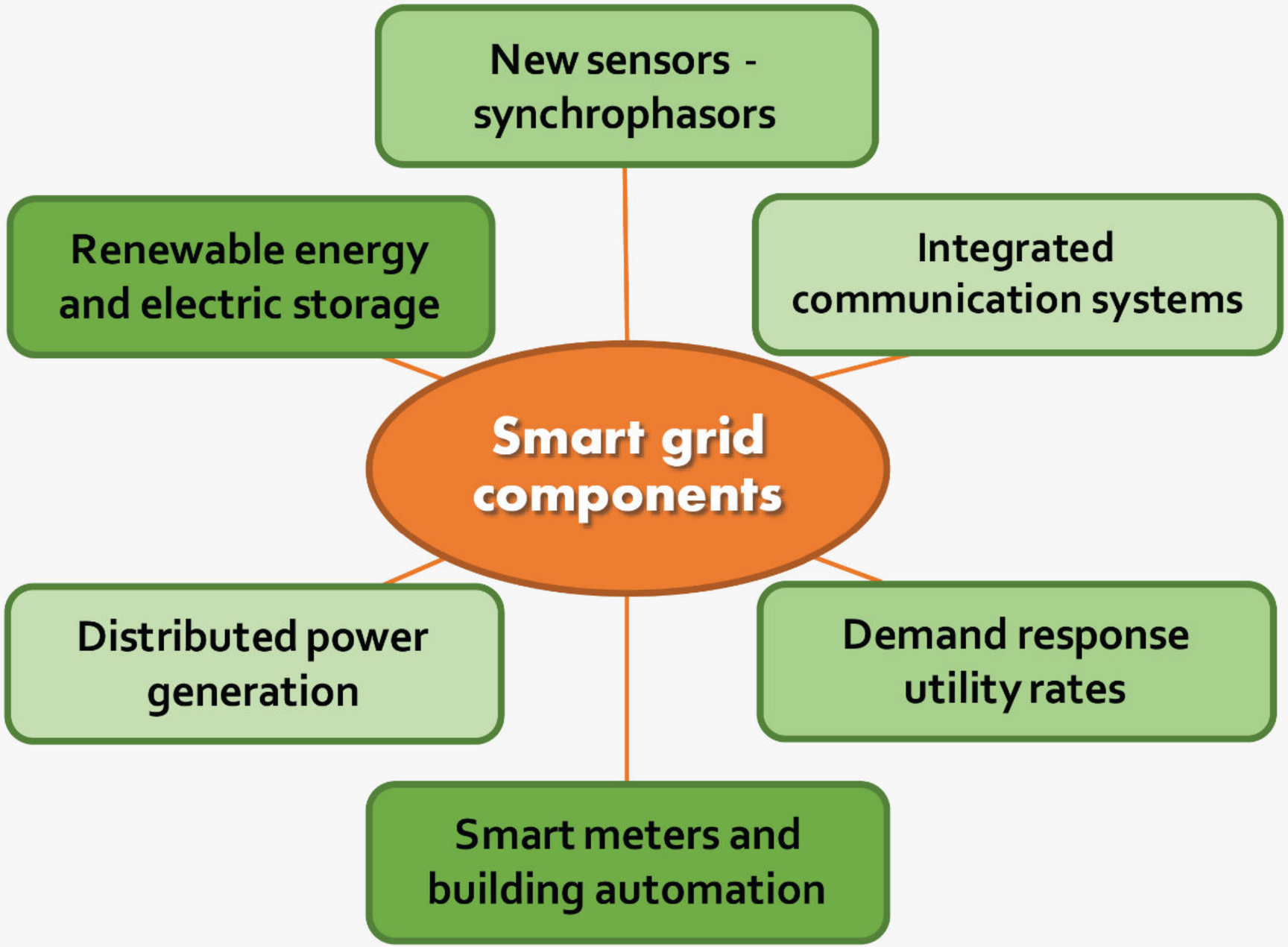



Interoperability Dimension
Business Layer
-regulatory and market structures
-policies
-business models
-products and services
-market parties
...
Function Layer
-functions
-services
...
Information Layer
-information objects
-data models
-semantics
-attacks
...
Communication Layer
-protocols
-specifications
-security measures
-implementation
-reliability
Component Layer
-design
-development
-production
-installation
-operation
-maintenance
-disposal
Outline of Usecase
Data Mod
Protoco
Generation
Transmission
Distribution

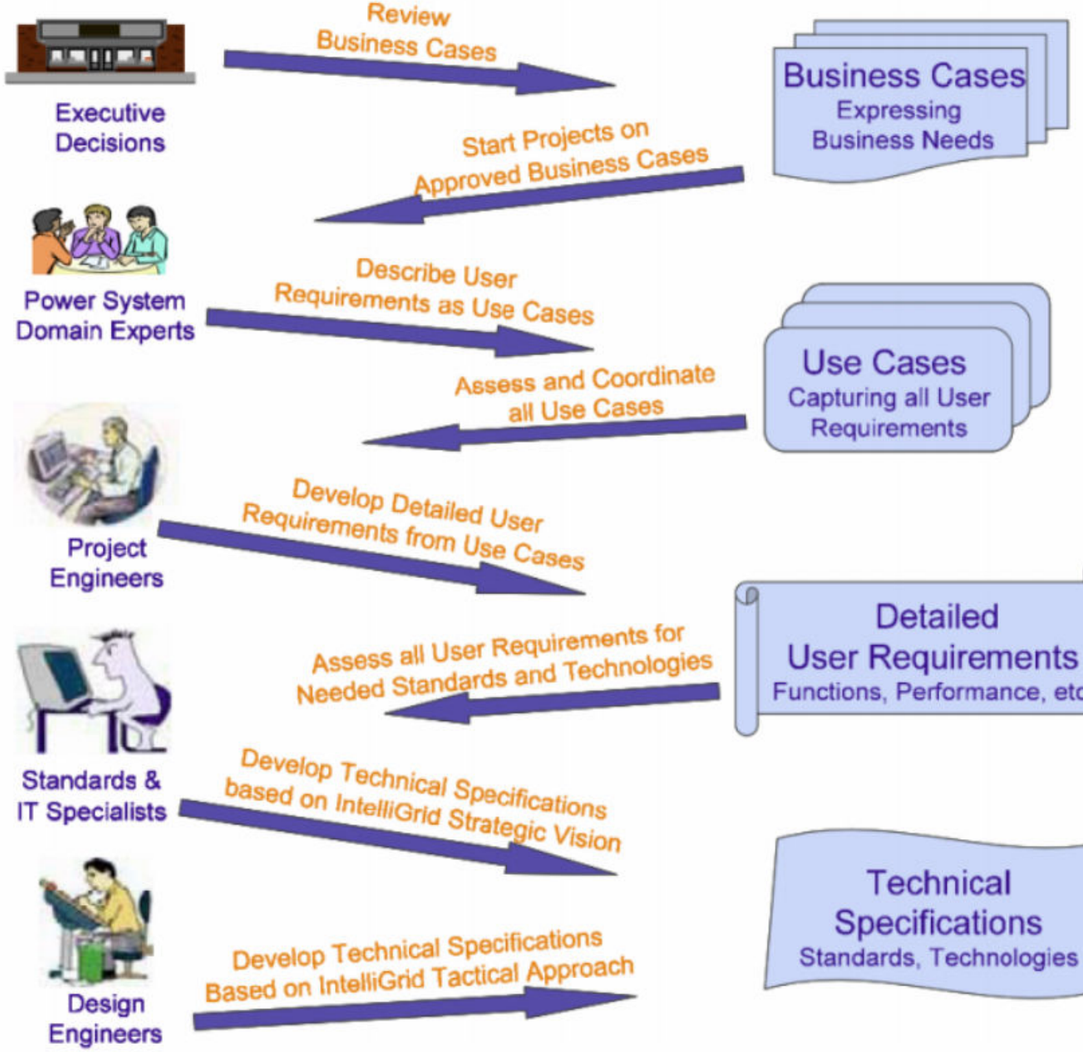


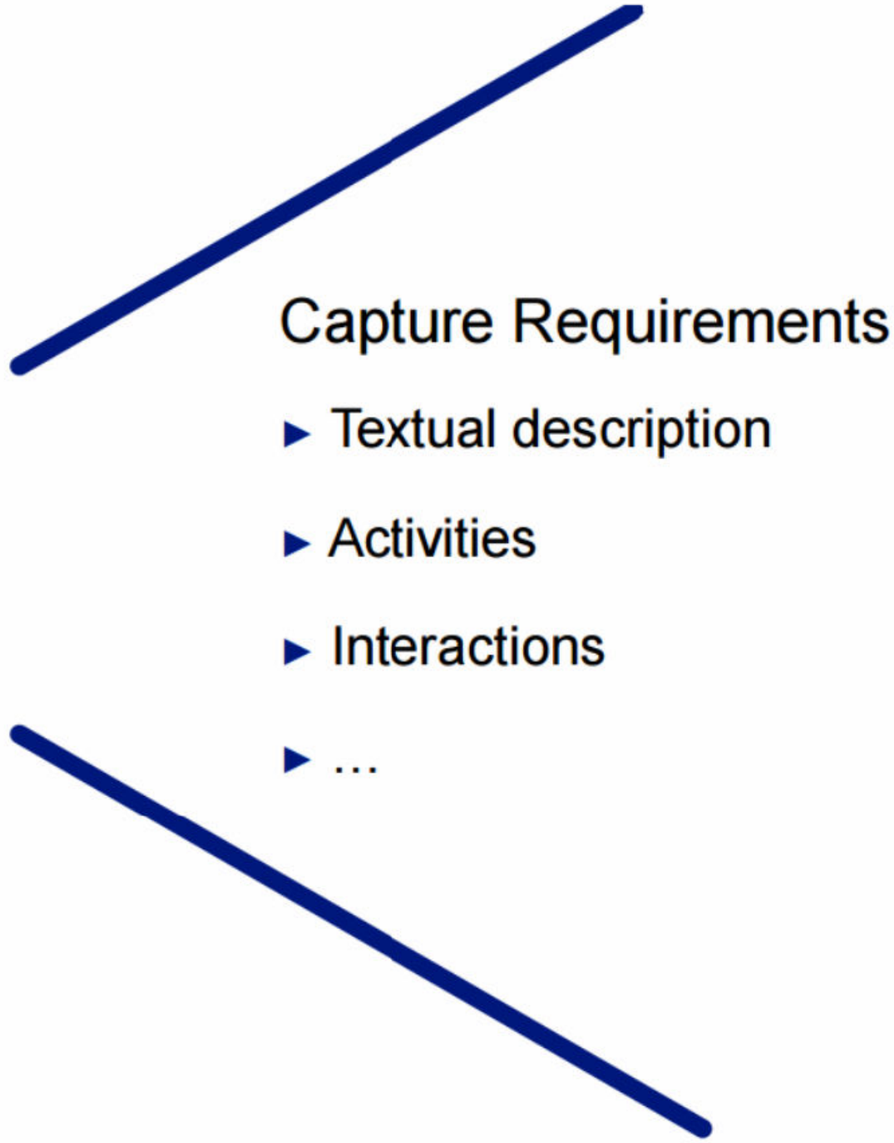
Human decisions and actions have an impact on every aspect of the system

Starting point: 1. Main challenges and opportunities



2. Use cases and related requirements extracted from existing literature





3. Table of requirements

No of chal-lenge	Source document	Requirement	Stakeholder(s) expressing or benefiting from the fulfillment of the requirement	Stakeholder(s) responsible for the fulfillment of the requirement
1	[10]	Maintain Grid stability and reliability during intermittent renewable source integration	Electricity consumers	Distribution System Operators, Distributed Generation Operators
2	[15]	Information and data exchange	Bulk Generation Operators, Transmission System Operators, Distribution System Operators, Service and Market Providers	Customers, Regulation Authorities and Politics
3	[16]	Compute forecast for renewable generation in controlled area based on weather forecast	Transmission System Operators, Distribution System Operators	Renewable Generation Forecaster
4	[16]	Utilization of electric vehicle battery for grid flexibility	Distribution System Operator	Electric vehicle user, Energy (e-Mobility) Service Operator
5	[15]	Override option at any time in Demand Response programs	Customer	Distribution System Operators
6	[15]	Harmonized and stable technical interconnection rules at national and EU level	Bulk Generation Operators, Transmission System Operators, Distribution System Operators	Regulation Authorities and Politics

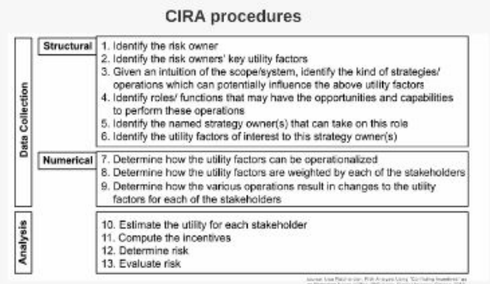
4. Identify key CIRA concepts:

Based on a specific requirement -> Define scope/ boundaries

Identify stakeholders:

-risk owner

-strategy owner(s)



Identify strategies (actions to increase perceived utility, modify risk owner's utility)

Identify utilities for each stakeholder:

-utility factors (e.g. wealth, reputation...)

CIRA procedures

Data Collection

Structural

1. Identify the risk owner
2. Identify the risk owners' key utility factors
3. Given an intuition of the scope/system, identify the kind of strategies/ operations which can potentially influence the above utility factors
4. Identify roles/ functions that may have the opportunities and capabilities to perform these operations
5. Identify the named strategy owner(s) that can take on this role
6. Identify the utility factors of interest to this strategy owner(s)

Numerical

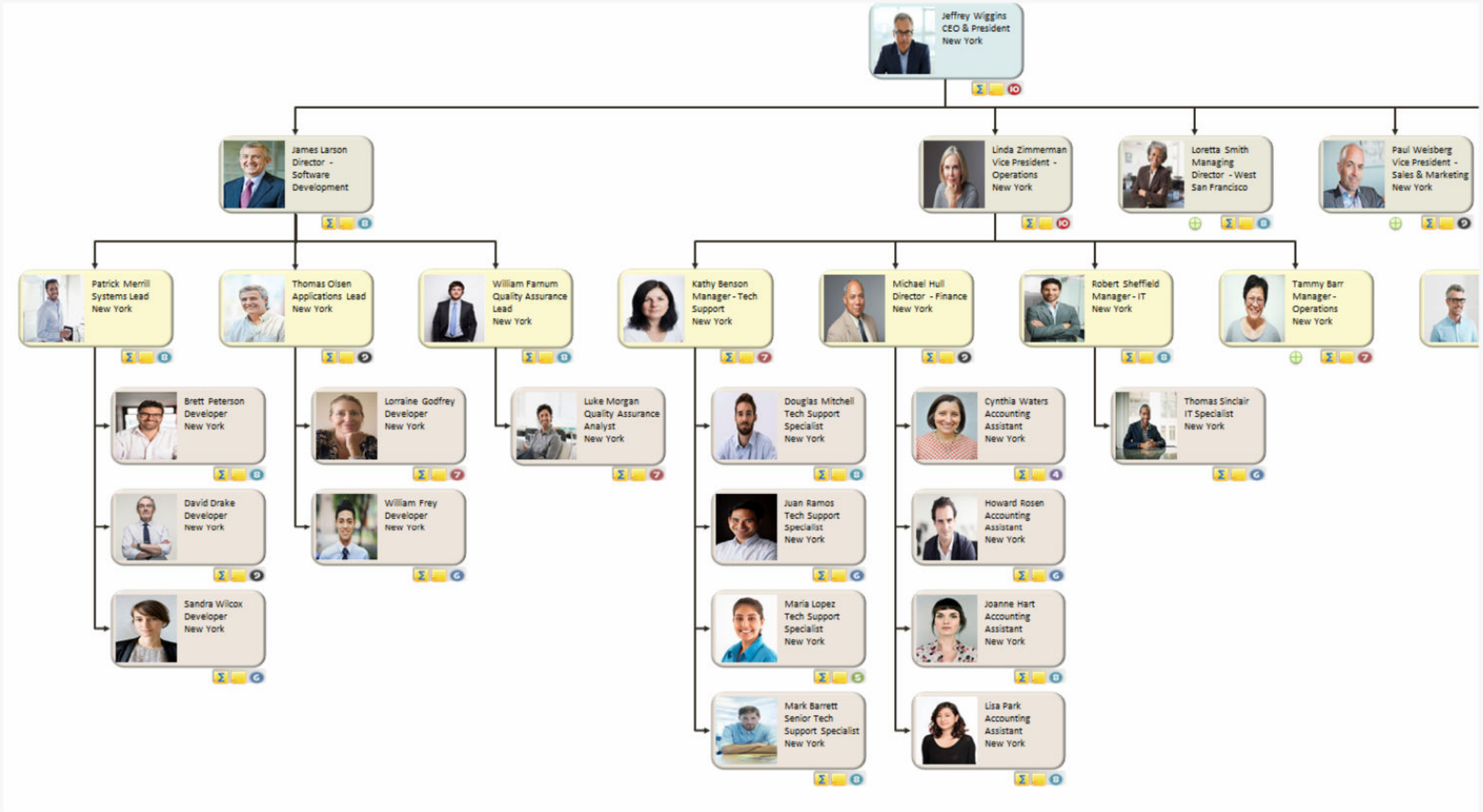
7. Determine how the utility factors can be operationalized
8. Determine how the utility factors are weighted by each of the stakeholders
9. Determine how the various operations result in changes to the utility factors for each of the stakeholders

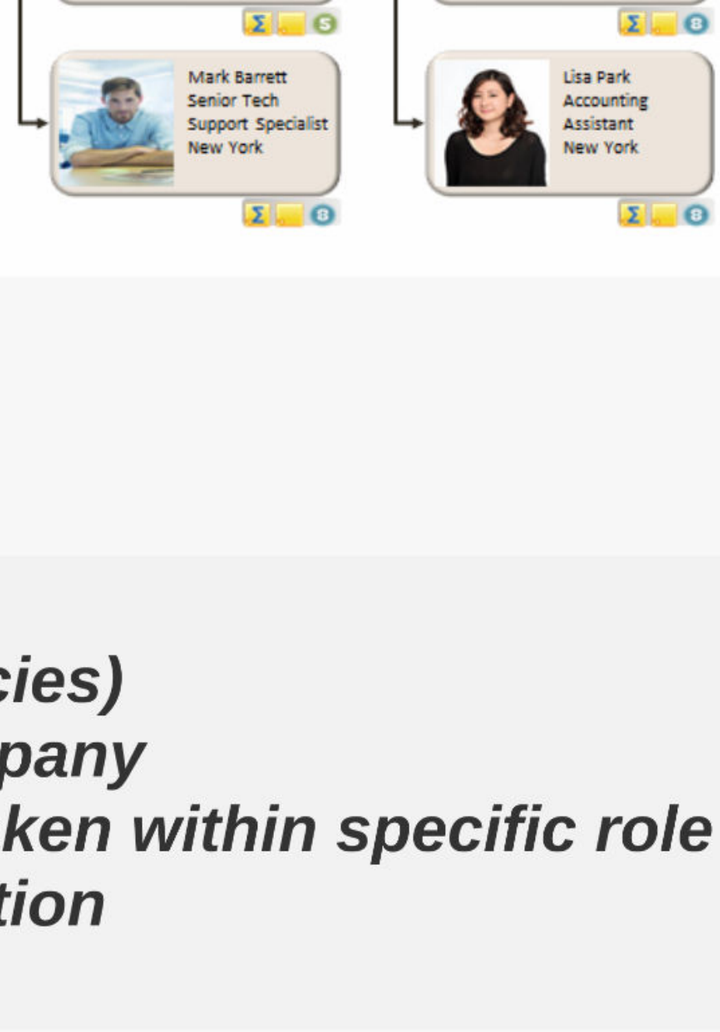
Analysis

10. Estimate the utility for each stakeholder
11. Compute the incentives
12. Determine risk
13. Evaluate risk

source: Lisa Rajbhandari. Risk Analysis Using "Conflicting Incentives" as an Alternative Notion of Risk. PhD thesis, Gjøvik University College, 2013.

5. Identify actual persons based on roles and associated responsibilities within a company





Focus on:

-chain of command (dependencies)
-incentive structure within company
-possible actions that can be taken within specific role
-individual's profile and motivation

6. Check whether stakeholder utilities are misaligned

Threat Risk - Opportunity Risk

Case study for demonstration - Threats during the Smart Meter's life cycle

Motivation:
-SM is key component of the Smart Grid
-widely implemented
-data about incidents

Dependencies

EU/Government directives

↓

DSO's responsibility to implement Smart Metering systems

↓

Comply with regulations (e.g. ensure customer privacy)

↓

Company/CEO goals (e.g. provide reliable supply of electricity, decrease operational cost, attract new customers, avoid the complexity and expense of implementing security in retrospect...)

↓

Find "proper" SM provider

Value chain of the Smart Meter

Security is not just about enabling the technical features on the smart meter but ensuring the underlying processes are managed in a secure and trusted way across the value chain

source: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5926

Silicon manufacturer → *Equipment manufacturer* → *Deployment* → *Operation* → *Decommission*

Silicon manufacturer

Strategies that may influence the risk owner's utility:

- unsecure processes during manufacturing/shipment
- attacker designs and manufactures microcontroller that looks and acts like genuine
- attacker intercepts shipment and loads fake bootloader

Equipment manufacturer

Strategies that may influence the risk owner's utility:

- SM vendors primarily manufacture through contract partners, often in countries different from where design occurs -> distinct external threats. Contract third parties gain deep access into system architecture, hardware, and software - underpaid workers might be easily bribed
- ensure robust architecture design, and engineering processes
- thorough testing procedures
- social engineering to convince line workers to share the secret keys loaded during the process - affect cryptography
- Prevent Insider Access to All Entry Points in a Meter: secure diagnostic/ debugging mode, serial ports, infrared interfaces

Deployment

Operation

Decommission

Motivation:

-SM is key component of the Smart Grid

-widely implemented

-data about incidents

Dependencies

Dependencies

EU/Government directives

↓

DSO's responsibility to implement Smart Metering systems

↓

Comply with regulations (e.g. ensure customer privacy)

↓

Company/CEO goals (e.g. provide reliable supply of electricity, decrease operational cost, attract new customers, avoid the complexity and expense of implementing security in retrospect...)

↓

Find "proper" SM provider

"In Northern Europe, four Norwegian power utilities have ordered 50,000 meters from manufacturer XY for a smart meter rollout." - 10 AUGUST 2015

What risks might the utility companies face?

http://www.metering.com/smart-meter-rollout-norway-utility-consortium-selects-kampstrup/

Value chain of the Smart Meter

Security is not just about enabling the technical features on the smart meter but ensuring the underlying processes are managed in a secure and trusted way across the value chain

source: https://www.maximintegrated.com/en/app-notes/index.mvp/id/5926

Silicon manufacturer

Strategies that may influence the risk owner's utility:

- unsecure processes during manufacturing/shipment
- attacker designs and manufactures microcontroller that looks and acts like genuine
- attacker intercepts shipment and loads fake bootloader

Identify roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within company to ensure safety?

-who is responsible for safe shipping?

Equipment manufacturer

The meter security breach in Puerto Rico occurred from tampering, possibly during the manufacturing process by former employees of the manufacturer

Strategies that may influence the risk owner's utility:

-SM vendors primarily manufacture through contract partners, often in countries different from where design occurs -> distinct external threats. Contract third parties gain deep access into system architecture, hardware, and software - underpaid workers might be easily bribed

- ensure robust architecture design, and engineering processes
- secure firmware (e.g. infected USB sticks' shipping from offshore factories)
- thorough testing procedures
- social engineering to convince line workers to share the secret keys loaded during the process - affect cryptography
- Prevent Insider Access to All Entry Points in a Meter: secure diagnostic/ debugging mode, serial ports, infrared interfaces

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within the company to ensure safety and who is responsible to enforce them?

Identify named strategy owners that can take on this role.

Deployment

Strategies that may influence the risk owner's utility:

-most utilities do not employ enough people to rapidly install the meters within an adequate period. Consequently, AMI installations typically require third-party contractors, which means that **third parties, again, are handling the critical meter infrastructure**. Physical hacking of optical ports, or simply rewiring meters, can occur during the installation process

- Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so. "These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters"

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-who is responsible for the reliability of personnel?

-who assesses the quality of work and how?

Identify named strategy owners that can take on this role.

Operation

Strategies that may influence the risk owner's utility:

- operation in high-risk locations, no physical protection
- SM stolen, taken to a lab, inspected by attacker
- recalibration with insider access to lower electricity bill/disguise consumption - on a large scale causes economic losses for the utility and disrupts network stability
- because of remote meter readings, detection of fraud is difficult
- economic benefit to both the hacker and the electric customer
- disrupt the quality of life for a large number of people - terrorists
- customer privacy concerns - delay in adoption
- attacker gets insight about customer's behavior by observing consumption signature

Roles that have the opportunity/capability to perform these operations:

-who has access to SM data?

-how to identify customers who might be motivated to tamper with consumption data?

-who would be motivated to tamper with reported data?

Identify named strategy owners that can take on this role.

Decommission

Strategies that may influence the risk owner's utility:

- Ensure all sensitive data (e.g. security credentials and personal information) is disposed of securely

Roles that have the opportunity/capability to perform these operations:

-who is liable if private consumer data is retrieved due to negligent handling of decommissioned SMs?

Identify named strategy owners that can take on this role.

Silicon manufacturer

Strategies that may influence the risk owner's utility:

- unsecure processes during manufacturing/shipment

- attacker designs and manufactures microcontroller that looks and acts like genuine

- attacker intercepts shipment and loads fake bootloader

Identify roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within company to ensure safety?

-who is responsible for safe shipping?

Equipment manufa

The meter security breach in Puerto Rico occurred tampering, possibly during the manufacturing proc former employees of the manufacturer

Strategies that may influence the risk owner's utility

-SM vendors primarily manufacture through contract countries different from where design occurs -> distin Contract third parties gain deep access into system a and software - underpaid workers might be easily bri

- ensure robust architecture design, and engineering

- secure firmware (e.g. infected USB sticks' shipping

- thorough testing procedures

- social engineering to convince line workers to share during the process - affect cryptography

- Prevent Insider Access to All Entry Points in a Mete debugging mode, serial ports, infrared interfaces

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within the company to ensure safety and who is responsible to enforce them?

- attacker intercepts shipment and loads fake bootloader

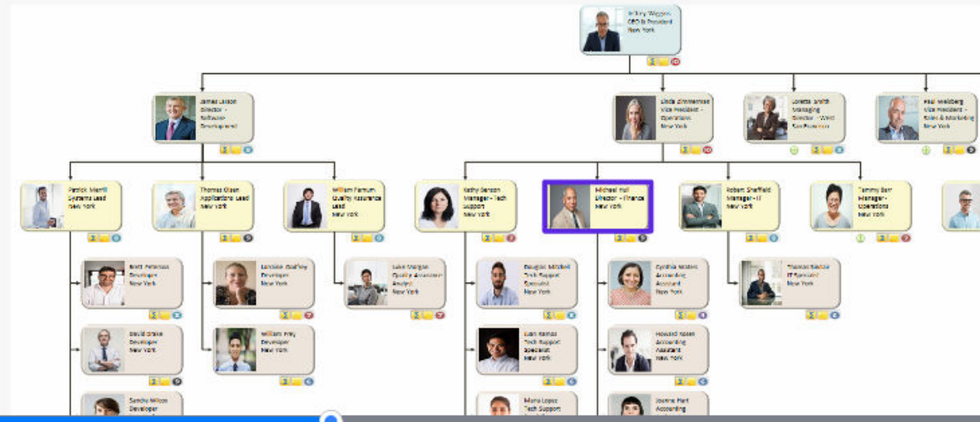
Identify roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

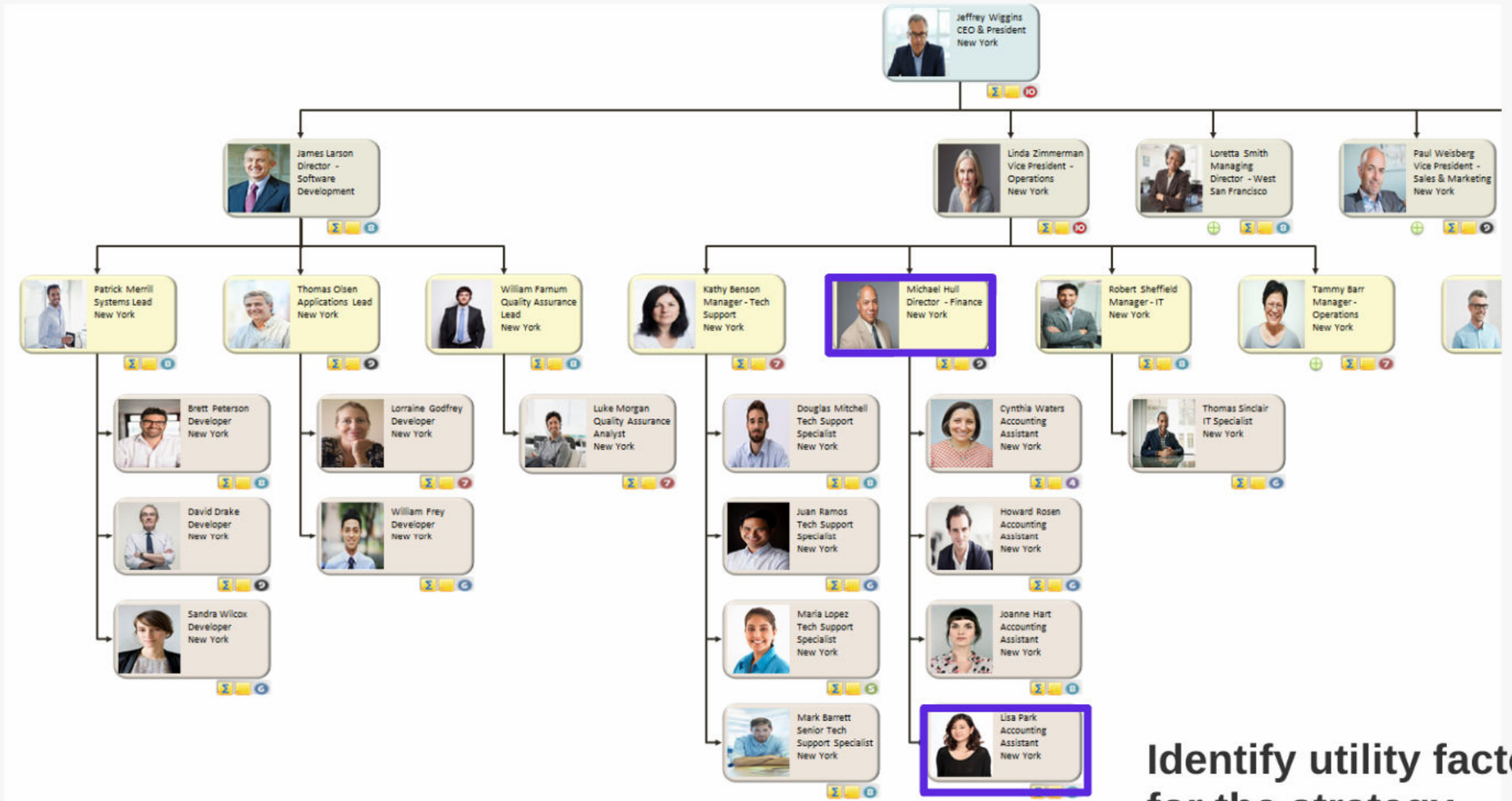
-what are the regulations within company to ensure safety?

-who is responsible for safe shipping?

Identify named strategy owners that can take on this role



Identify named strategy owners that can take on this role



Identify utility factors for the strategy owner -> predict likely behavior

con manufacturer

t may influence the risk owner's utility:

processes during manufacturing/shipment

esigns and manufactures microcontroller
nd acts like genuine

tercepts shipment and loads fake

have the opportunity/capability to
rations:

ble for ensuring the safety of

gulations within company to ensure

ble for safe shipping?

Equipment manufacturer

The meter security breach in Puerto Rico occurred from tampering, possibly during the manufacturing process by former employees of the manufacturer

source: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

Strategies that may influence the risk owner's utility:

-SM vendors primarily manufacture through contract partners, often in countries different from where design occurs -> distinct external threats. Contract third parties gain deep access into system architecture, hardware, and software - underpaid workers might be easily bribed

- ensure robust architecture design, and engineering processes

- secure firmware (e.g. infected USB sticks' shipping from offshore factories)

- thorough testing procedures

- social engineering to convince line workers to share the secret keys loaded during the process - affect cryptography

- Prevent Insider Access to All Entry Points in a Meter: secure diagnostic/ debugging mode, serial ports, infrared interfaces

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within the company to ensure safety and who is responsible to enforce them?

Deployment

Strategies that may influence the risk owner's utility:

-most utilities do not employ enough people to rapidly install meters within an adequate period. Consequently, AMI install typically require third-party contractors, which means that **th parties, again, are handling the critical meter infrastruct** Physical hacking of optical ports, or simply rewiring meters, during the installation process

- Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the were altering the meters in exchange for cash and training c do so. “These individuals are charging $300 to $1,000 to rep residential meters, and about $3,000 to reprogram commerc meters”

Roles that have the opportunity/capability to perform these operati

-who is responsible for ensuring the safety of operations?

-who is responsible for the reliability of personnel?

-who assesses the quality of work and how?

- Prevent Insider Access to All Entry Points in a Me
debugging mode, serial ports, infrared interfaces

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-what are the regulations within the company to ensure safety and who is responsible to enforce them?

Identify named strategy owners that can take on this role.

uipment manufacturer

The meter security breach in Puerto Rico occurred from tampering, possibly during the manufacturing process by former employees of the manufacturer

source: http://krebsonsecurity.com/2012/04/fbi-smart-meter-hacks-likely-to-spread/

may influence the risk owner's utility:

primarily manufacture through contract partners, often in
rent from where design occurs -> distinct external threats.
parties gain deep access into system architecture, hardware,
underpaid workers might be easily bribed

st architecture design, and engineering processes

are (e.g. infected USB sticks' shipping from offshore factories)

ting procedures

eering to convince line workers to share the secret keys loaded
cess - affect cryptography

der Access to All Entry Points in a Meter: secure diagnostic/
de, serial ports, infrared interfaces

rtunity/capability to perform these operations:

ensuring the safety of operations?

ns within the company to ensure safety and who is
them?

Deployment

Strategies that may influence the risk owner's utility:

-most utilities do not employ enough people to rapidly install the meters within an adequate period. Consequently, AMI installations typically require third-party contractors, which means that **third parties, again, are handling the critical meter infrastructure**. Physical hacking of optical ports, or simply rewiring meters, can occur during the installation process

- Citing confidential sources, the FBI said it believes former employees of the meter manufacturer and employees of the utility were altering the meters in exchange for cash and training others to do so. “These individuals are charging $300 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters”

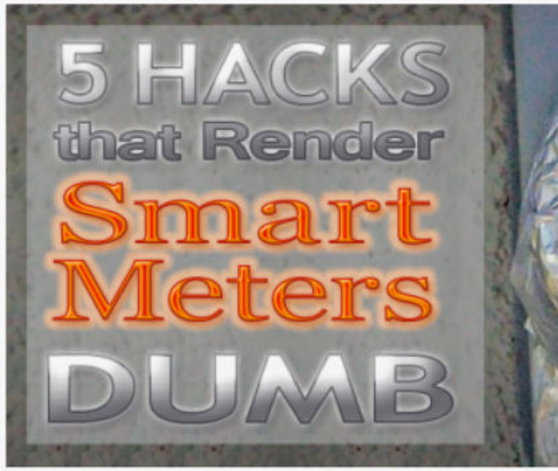
Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-who is responsible for the reliability of personnel?

-who assesses the quality of work and how?

Operati



Strategies that may influence the risk owner's utility:

- operation in high-risk locations, no physical protecti

- SM stolen, taken to a lab, inspected by attacker

- recalibration with insider access to lower electricity b
economic losses for the utility and disrupts network st

- because of remote meter readings, detection of frau

- economic benefit to both the hacker and the electric

- disrupt the quality of life for a large number of peopl

- customer privacy concerns - delay in adoption

- attacker gets insight about customer's behavior by c

Roles that have the opportunity/capability to perform these oper

-who has access to SM data?

-how to identify customers who might be motivated to tamper with
consumption data?

-who would be motivated to tamper with reported data?

do so.” These individuals are charging $500 to $1,000 to reprogram residential meters, and about $3,000 to reprogram commercial meters”

Roles that have the opportunity/capability to perform these operations:

-who is responsible for ensuring the safety of operations?

-who is responsible for the reliability of personnel?

-who assesses the quality of work and how?

Identify named strategy owners that can take on this role.

...loyment

...he risk owner's utility:

...nough people to rapidly install the ...riod. Consequently, AMI installations ...ntractors, which means that **third the critical meter infrastructure**. ...rts, or simply rewiring meters, can occur

...he FBI said it believes former ...facturer and employees of the utility ...change for cash and training others to ...charging $300 to $1,000 to reprogram ...$3,000 to reprogram commercial

...apability to perform these operations:

...the safety of operations?

...ility of personnel?

...k and how?

Operation

Strategies that may influence the risk owner's utility:

- operation in high-risk locations, no physical protection

- SM stolen, taken to a lab, inspected by attacker

- recalibration with insider access to lower electricity bill/disguise consumption - on a large scale causes economic losses for the utility and disrupts network stability

- because of remote meter readings, detection of fraud is difficult

- economic benefit to both the hacker and the electric customer

- disrupt the quality of life for a large number of people - terrorists

- customer privacy concerns - delay in adoption

- attacker gets insight about customer's behavior by observing consumption signature

Roles that have the opportunity/capability to perform these operations:

-who has access to SM data?

-how to identify customers who might be motivated to tamper with consumption data?

-who would be motivated to tamper with reported data?

Decommiss

Strategies that may influence the risk owner's ut

- Ensure all sensitive data (e.g. security credenti disposed of securely

Roles that have the opportunity/capability to per

-who is liable if private consumer data is retrieve decommissioned SMs?

Identify named strategy owners that can take on

- customer privacy concerns - delay in adoption

- attacker gets insight about customer's behavior by observing consumption s

Roles that have the opportunity/capability to perform these operations:

-who has access to SM data?

-how to identify customers who might be motivated to tamper with consumption data?

-who would be motivated to tamper with reported data?

Identify named strategy owners that can take on this role.

Decommission

sumption - on a large scale causes

Strategies that may influence the risk owner's utility:

- Ensure all sensitive data (e.g. security credentials and personal information) is disposed of securely

Roles that have the opportunity/capability to perform these operations:

-who is liable if private consumer data is retrieved due to negligent handling of decommissioned SMs?

Identify named strategy owners that can take on this role


Next steps...