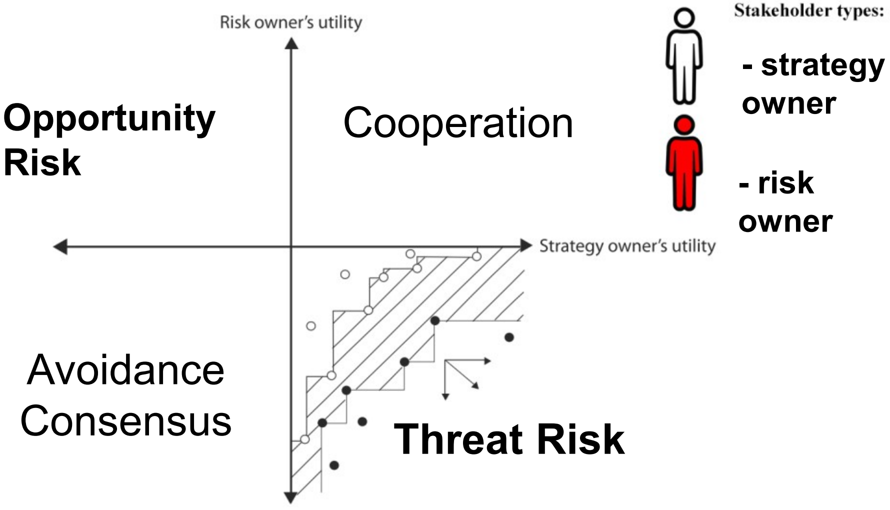
NTNU

IoTSec meeting

Adam Szekeres
NTNU Gjøvik
24.10.2019
- how each partner contributes to the overall goals of the project?

Main objective: enhance the Conflicting Incentives Risk Analysis (CIRA) method

Starting point:
theoretical foundations



Opportunity Risk

Cooperation

Avoidance Consensus

Threat Risk

Stakeholder types:

- strategy owner

- risk owner

Desired goal:
Real stakeholders in real scenarios, using observation only to

Analyze risks

Motivation

Motivation

Motivation

Motivation

Motivation

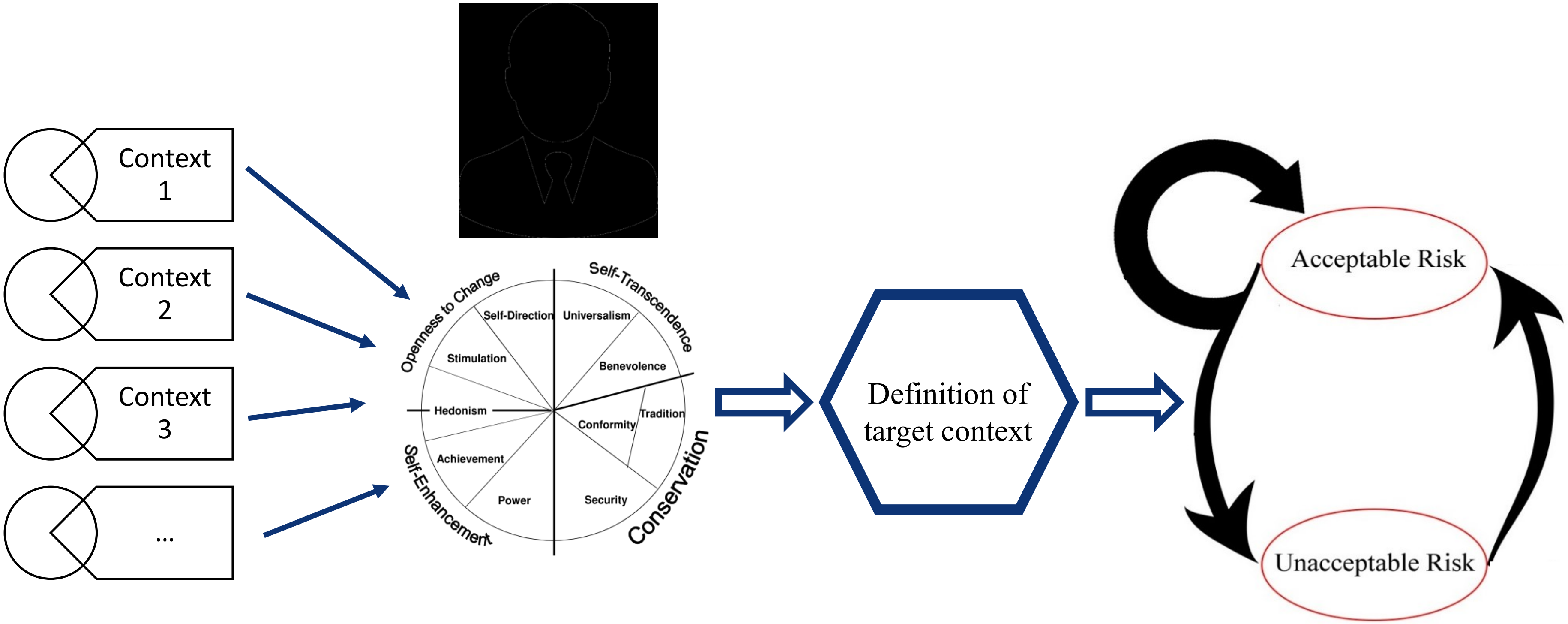
Motivation

Motivation

Motivation

Motivation

Human motivation and the security of IoT



1. Observation of past choices in various contexts

2. Profile creation

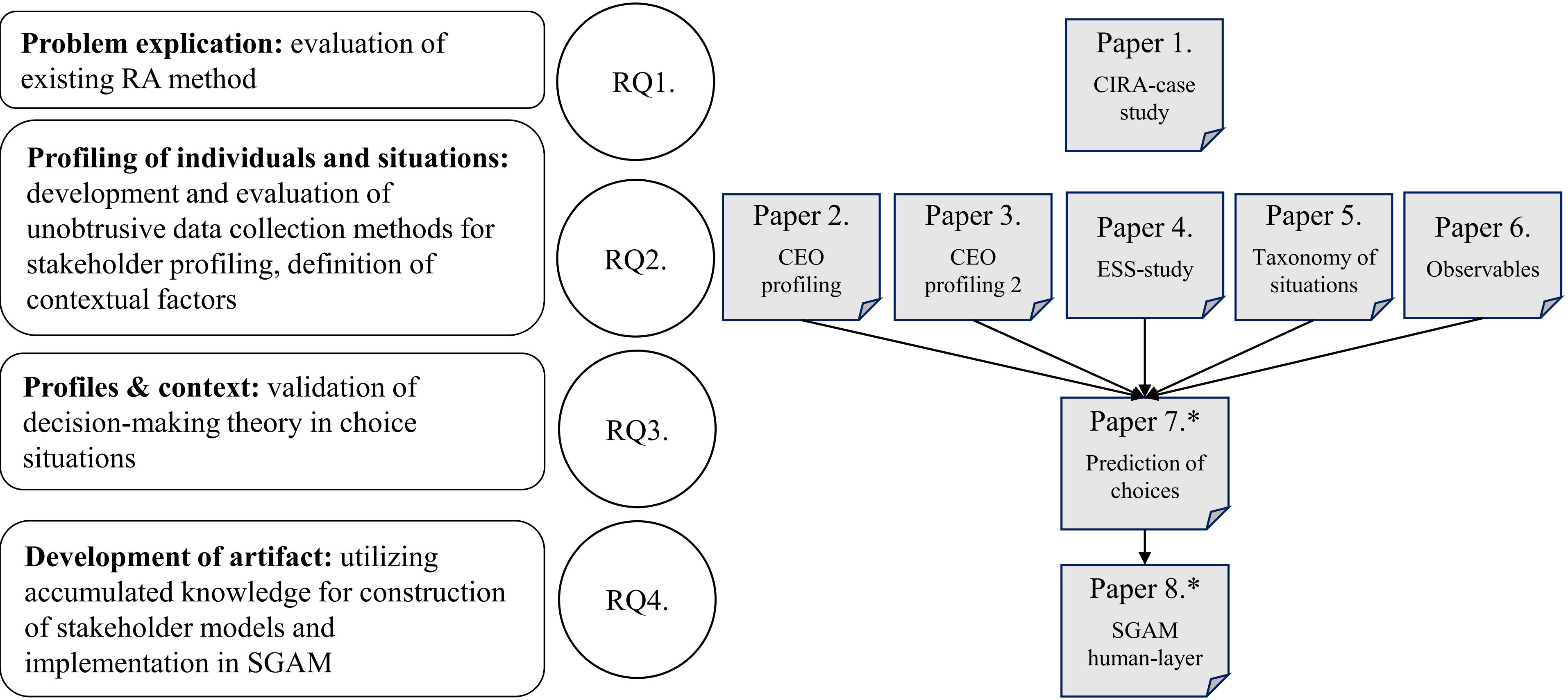
3. Prediction of decisions in target context

4. Analyze risks resulting from conscious (System 2) decisions

How to improve the **CIRA** method by using theories from psychology which enable the **prediction of future behavior** of key stakeholders, **without** relying on **reactive data collection methods**?

Make the method **applicable for Smart Grid scenarios**.

Connection of objectives, research questions and papers



Problem explication: evaluation of existing RA method

Profiling of individuals and situations: development and evaluation of unobtrusive data collection methods for stakeholder profiling, definition of contextual factors

Profiles & context: validation of decision-making theory in choice situations

Development of artifact: utilizing accumulated knowledge for construction of stakeholder models and implementation in SGAM

RQ1.

RQ2.

RQ3.

RQ4.

Paper 1. CIRA-case study

Paper 2. CEO profiling

Paper 3. CEO profiling 2

Paper 4. ESS-study

Paper 5. Taxonomy of situations

Paper 6. Observables

Paper 7.* Prediction of choices

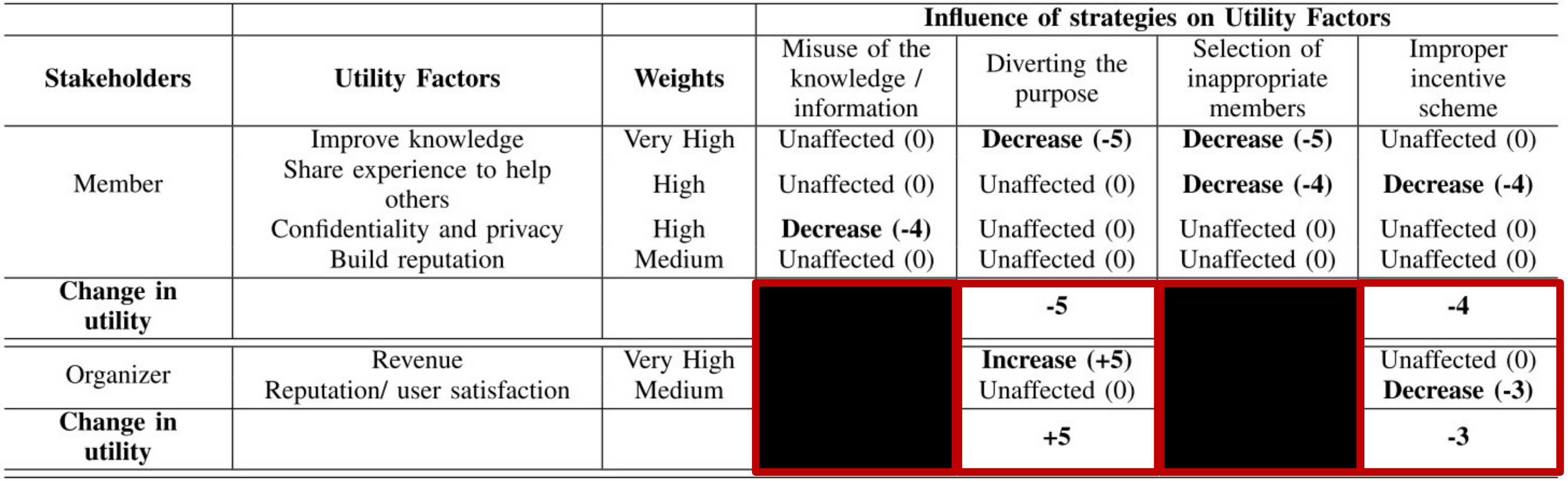
Paper 8.* SGAM human-layer

* Papers need finalizing

Research Questions

- RQ 1: What are the capabilities and limitations of the existing CIRA method, when real-world application is considered?
- RQ 2: Which data collection methods can be efficiently utilized for building stakeholder profiles, taking into account the limited access to subjects during risk analysis?
- RQ 3: To what extent is the proposed framework able to predict actual choices?
- RQ 4: What are the advantages/disadvantages of an improved Smart Grid Architecture Model when performing a CIRA type of risk analysis?

Paper 1. - CIRA-case study



			Influence of strategies on Utility Factors			
Stakeholders	**Utility Factors**	**Weights**	Misuse of the knowledge / information	Diverting the purpose	Selection of inappropriate members	Improper incentive scheme
Member	Improve knowledge	Very High	Unaffected (0)	**Decrease (-5)**	**Decrease (-5)**	Unaffected (0)
	Share experience to help others	High	Unaffected (0)	Unaffected (0)	**Decrease (-4)**	**Decrease (-4)**
	Confidentiality and privacy	High	**Decrease (-4)**	Unaffected (0)	Unaffected (0)	Unaffected (0)
	Build reputation	Medium	Unaffected (0)	Unaffected (0)	Unaffected (0)	Unaffected (0)
Change in utility			[redacted]	**-5**	[redacted]	**-4**
Organizer	Revenue	Very High	[redacted]	**Increase (+5)**	[redacted]	Unaffected (0)
	Reputation/ user satisfaction	Medium	[redacted]	Unaffected (0)	[redacted]	**Decrease (-3)**
Change in utility			[redacted]	**+5**	[redacted]	**-3**

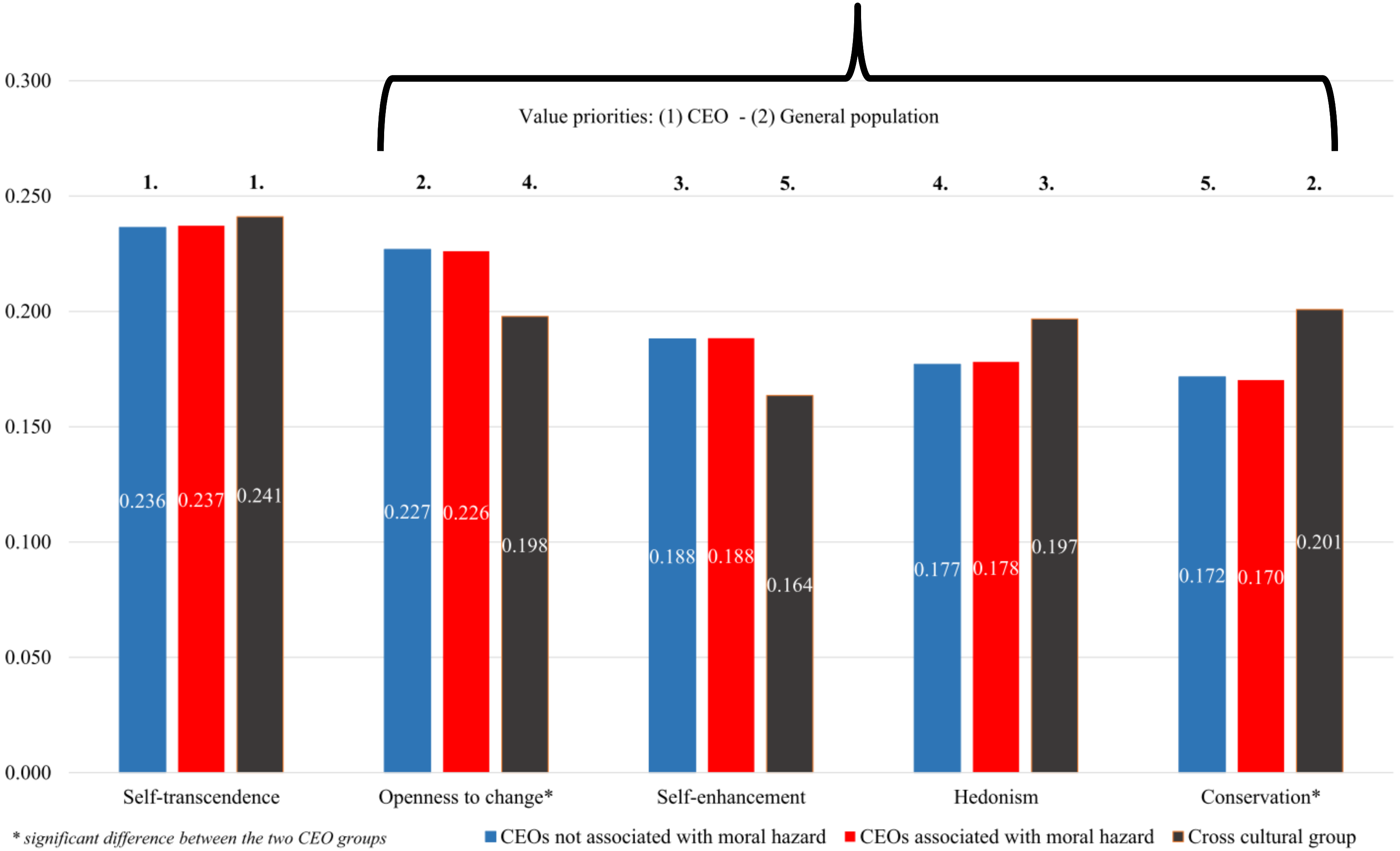
What are the capabilities and limitations of the existing CIRA method, when real-world application is considered?

Development of risk mitigation strategies in a community of practice setting, relying on direct data collection.

Evaluation of existing method’s capabilities.

Paper 2. - CEO profiling

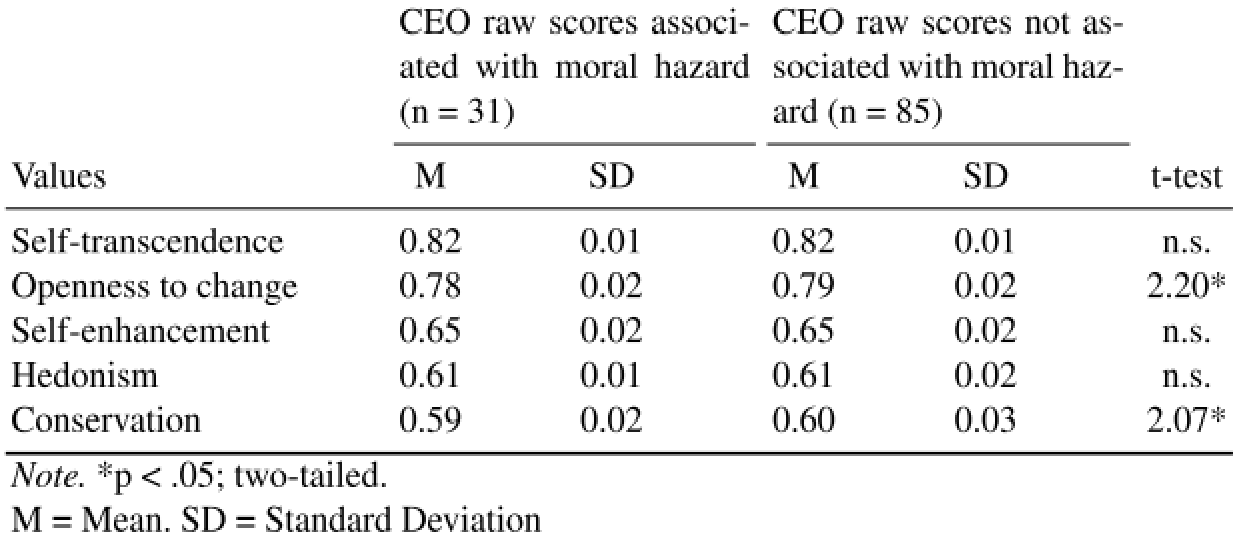
Evidence of selection-bias, feasibility of using interview data for profile building



** significant difference between the two CEO groups*

Paper 3. - CEO profiling 2

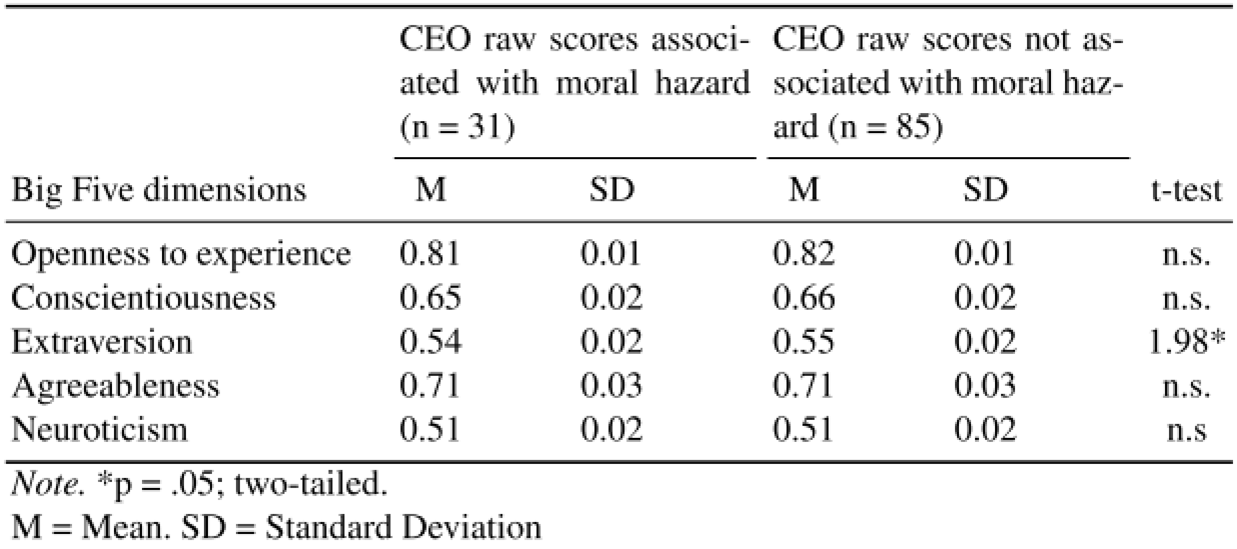
Basic Human values



Values	CEO raw scores associated with moral hazard (n = 31)		CEO raw scores not associated with moral hazard (n = 85)		
	M	SD	M	SD	t-test
Self-transcendence	0.82	0.01	0.82	0.01	n.s.
Openness to change	0.78	0.02	0.79	0.02	2.20*
Self-enhancement	0.65	0.02	0.65	0.02	n.s.
Hedonism	0.61	0.01	0.61	0.02	n.s.
Conservation	0.59	0.02	0.60	0.03	2.07*

Note. *p < .05; two-tailed.
M = Mean. SD = Standard Deviation

Big Five model of personality

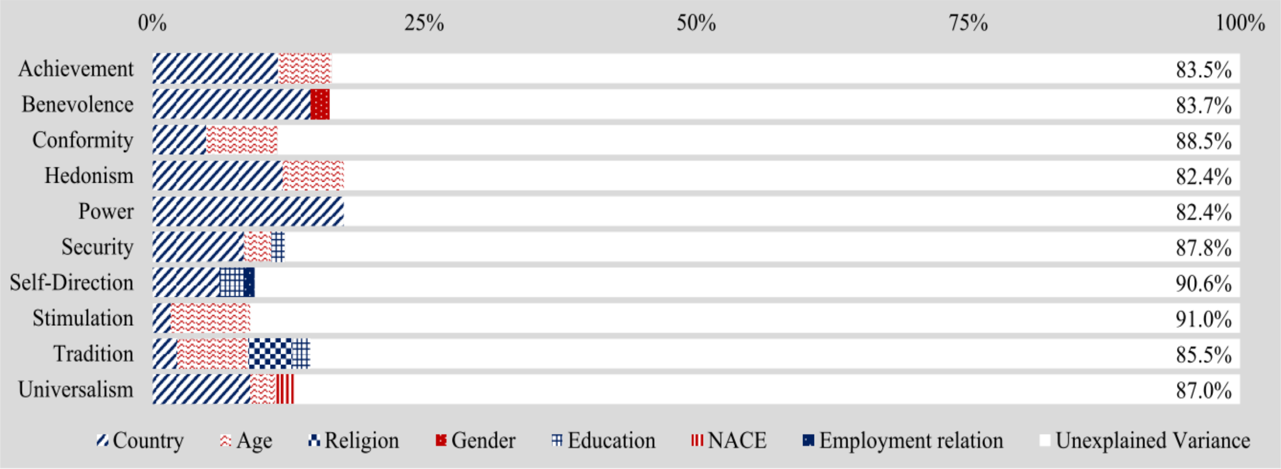


Big Five dimensions	CEO raw scores associated with moral hazard (n = 31)		CEO raw scores not associated with moral hazard (n = 85)		
	M	SD	M	SD	t-test
Openness to experience	0.81	0.01	0.82	0.01	n.s.
Conscientiousness	0.65	0.02	0.66	0.02	n.s.
Extraversion	0.54	0.02	0.55	0.02	1.98*
Agreeableness	0.71	0.03	0.71	0.03	n.s.
Neuroticism	0.51	0.02	0.51	0.02	n.s

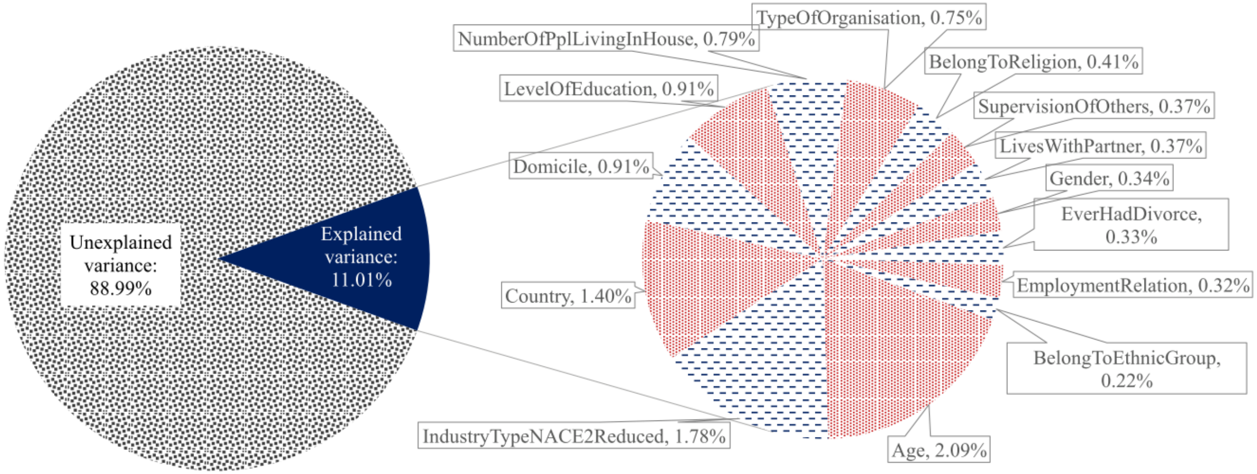
Note. *p = .05; two-tailed.
M = Mean. SD = Standard Deviation

Paper 4. - ESS-study

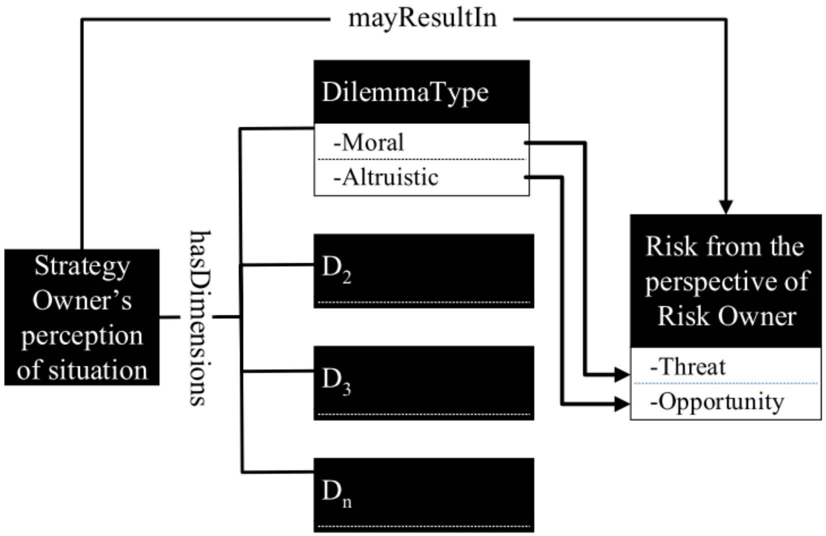
Multiple Linear Regression



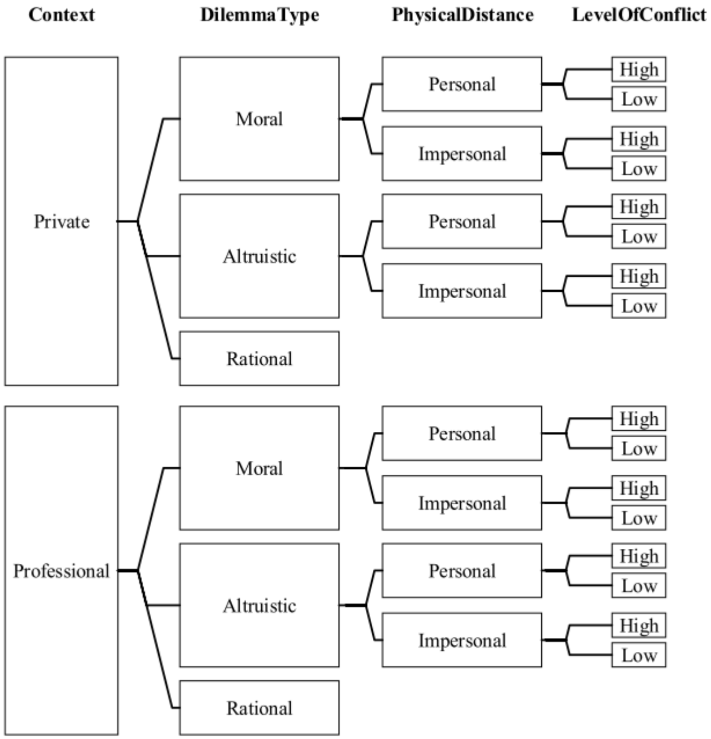
Machine Learning solution



Paper 5. - Taxonomy of situations



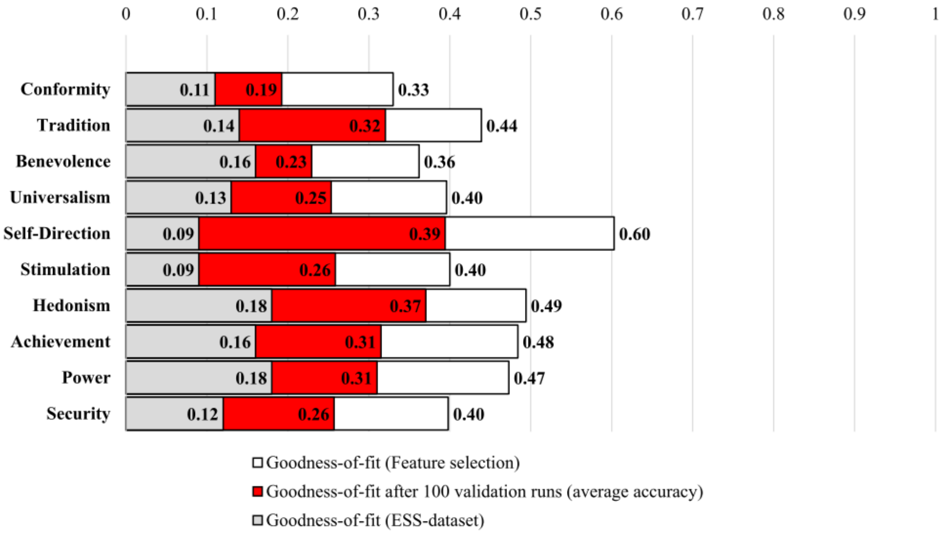
A mapping between CIRA risk-concepts and dilemma types in the literature



Taxonomy enables:
- classification of existing dilemmas
- generation of novel dilemmas

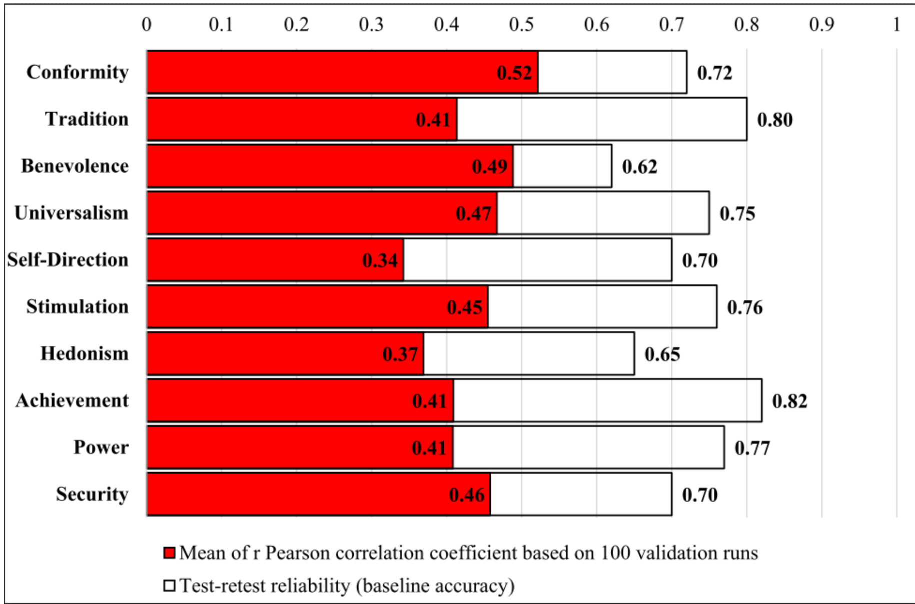
In a systematic, principled way

Paper 6. – Profiles from observables



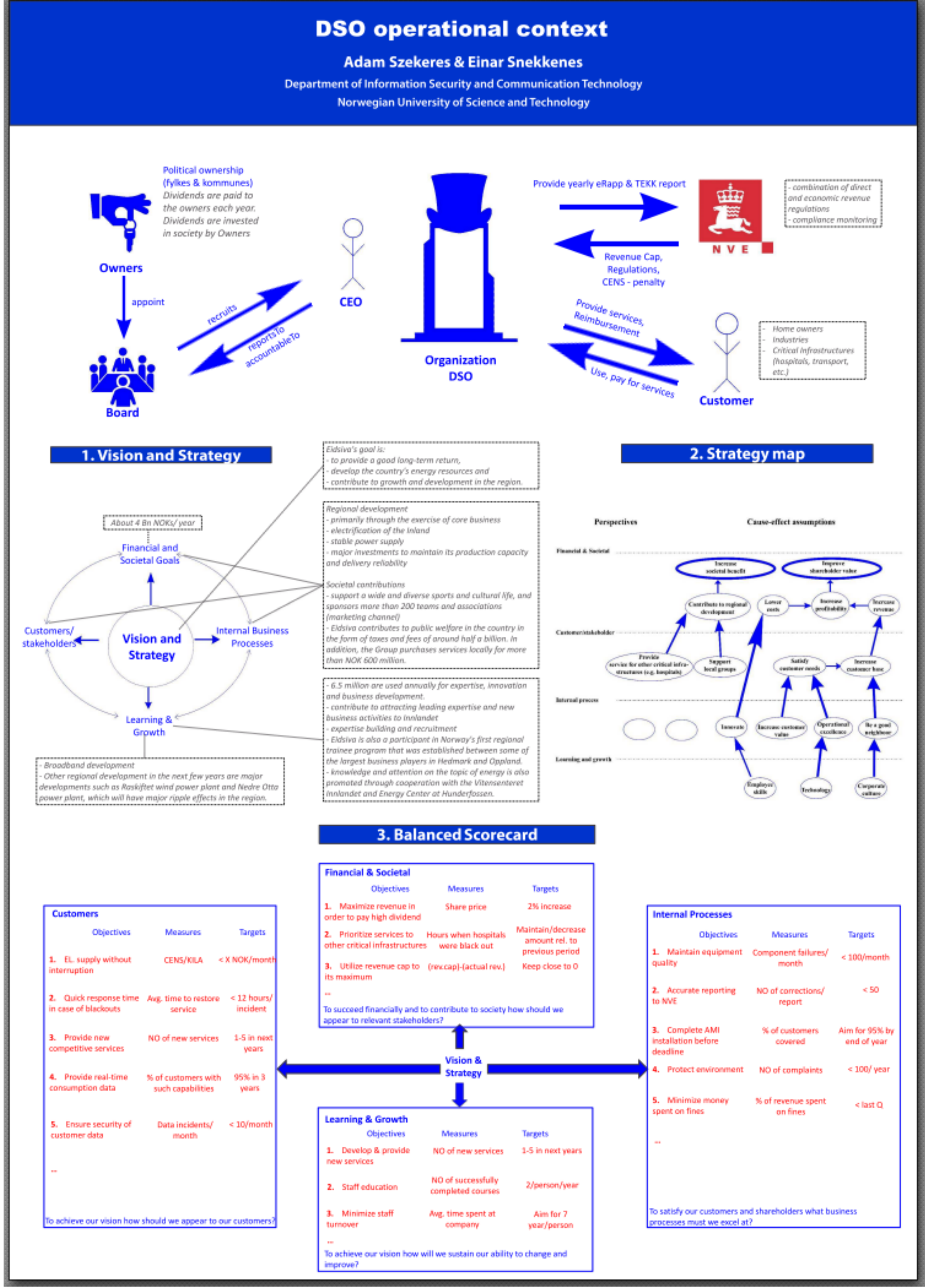
On average 3-fold improvement from baseline using other classes of observables

Prediction accuracy vs. questionnaires own accuracy



Other IoTSec-related activities toward common goal

Development of BSC to capture decision-makers context, create quantifiable metrics along which they may optimize their behavior.



DSO operational context

Adam Szekeres & Einar Snekkenes

Department of Information Security and Communication Technology
Norwegian University of Science and Technology

Political ownership
(fylkes & kommunes)
Owners
appoint
Board
recruits
reportsTo
accountableTo
CEO
Organization
DSO
Provide yearly eRapp & TEKK report
Revenue Cap,
Regulations,
CENS - penalty
N V E
Provide services,
Reimbursement
Use, pay for services
Customer

Dividends are paid to the owners each year. Dividends are invested in society by Owners

- combination of direct and economic revenue regulations
- compliance monitoring

- Home owners
- Industries
- Critical infrastructures (hospitals, transport, etc.)

1. Vision and Strategy

Eidsiva's goal is:
- to provide a good long-term return,
- develop the country's energy resources and
- contribute to growth and development in the region.

Regional development
- primarily through the exercise of core business
- electrification of the Inland
- stable power supply
- major investments to maintain its production capacity and delivery reliability

Societal contributions
- support a wide and diverse sports and cultural life, and sponsors more than 200 teams and associations (marketing channel)
- Eidsiva contributes to public welfare in the country in the form of taxes and fees of around half a billion. In addition, the Group purchases services locally for more than NOK 600 million.

- 6.5 million are used annually for expertise, innovation and business development.
- contribute to attracting leading expertise and new business activities to Innlandet
- expertise building and recruitment
- Eidsiva is also a participant in Norway's first regional trainee program that was established between some of the largest business players in Hedmark and Oppland.
- knowledge and attention on the topic of energy is also promoted through cooperation with the Vitensenteret Innlandet and Energy Center at Hunderfossen.

- Broadband development
- Other regional development in the next few years are major developments such as Raskiftet wind power plant and Nedre Otta power plant, which will have major ripple effects in the region.

2. Strategy map

3. Balanced Scorecard

Financial & Societal

Objectives	Measures	Targets
1. Maximize revenue in order to pay high dividend	Share price	2% increase
2. Prioritize services to other critical infrastructures	Hours when hospitals were black out	Maintain/decrease amount rel. to previous period
3. Utilize revenue cap to its maximum	(rev.cap)-(actual rev.)	Keep close to 0
...		

To succeed financially and to contribute to society how should we appear to relevant stakeholders?

Customers

Objectives	Measures	Targets
1. EL. supply without interruption	CENS/KILA	< X NOK/month
2. Quick response time in case of blackouts	Avg. time to restore service	< 12 hours/ incident
3. Provide new competitive services	NO of new services	1-5 in next years
4. Provide real-time consumption data	% of customers with such capabilities	95% in 3 years
5. Ensure security of customer data	Data incidents/ month	< 10/month
...		

To achieve our vision how should we appear to our customers?

Vision & Strategy

Internal Processes

Objectives	Measures	Targets
1. Maintain equipment quality	Component failures/ month	< 100/month
2. Accurate reporting to NVE	NO of corrections/ report	< 50
3. Complete AMI installation before deadline	% of customers covered	Aim for 95% by end of year
4. Protect environment	NO of complaints	< 100/ year
5. Minimize money spent on fines	% of revenue spent on fines	< last Q
...		

To satisfy our customers and shareholders what business processes must we excel at?

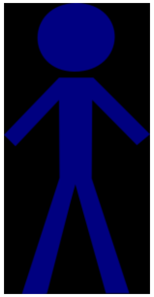
Learning & Growth

Objectives	Measures	Targets
1. Develop & provide new services	NO of new services	1-5 in next years
2. Staff education	NO of successfully completed courses	2/person/year
3. Minimize staff turnover	Avg. time spent at company	Aim for 7 year/person
...		

To achieve our vision how will we sustain our ability to change and improve?

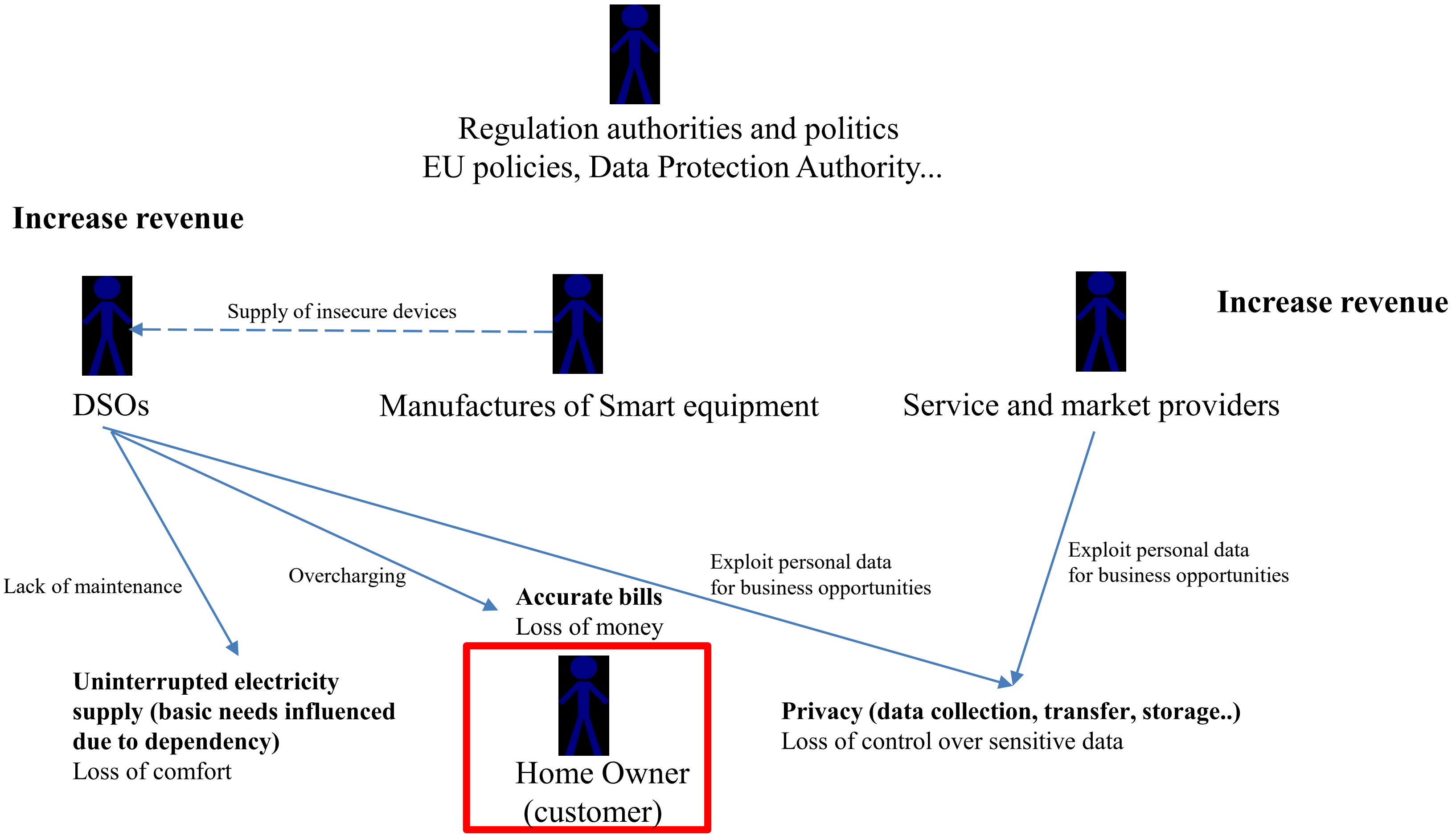
Proposed various common scenarios using the stakeholder model

- Set of Utility Factors (UF)
  - capture an aspect of utility (importance for decision maker)
  - Initial Value – representing current state
  - Final Value – representing desired end-state
- Set of strategies that the stakeholder considers
  - strategy allows the transition from current state to desired end-state



- Mental operation that selects a strategy to maximize utility

Scenario 1. – Customer as Risk Owner



Regulation authorities and politics
EU policies, Data Protection Authority...

Increase revenue

DSOs

Supply of insecure devices

Manufactures of Smart equipment

Service and market providers

Increase revenue

Lack of maintenance

Overcharging

Exploit personal data
for business opportunities

Exploit personal data
for business opportunities

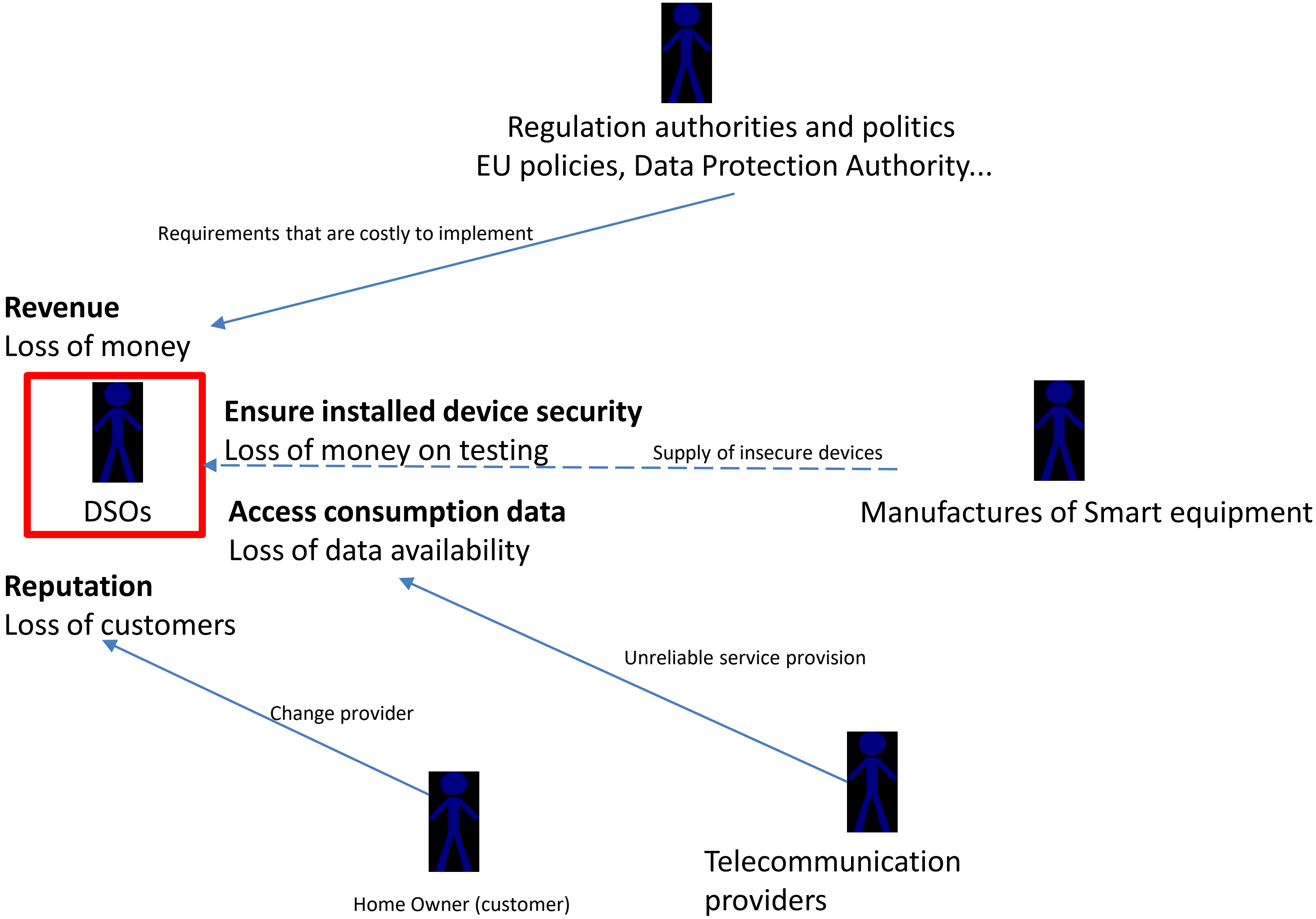
Accurate bills
Loss of money

Uninterrupted electricity supply (basic needs influenced due to dependency)
Loss of comfort

Home Owner
(customer)

Privacy (data collection, transfer, storage..)
Loss of control over sensitive data

Scenario 2. – DSO as Risk Owner



Regulation authorities and politics
EU policies, Data Protection Authority...

Requirements that are costly to implement

Revenue
Loss of money

DSOs

Ensure installed device security
Loss of money on testing

Supply of insecure devices

Manufactures of Smart equipment

Access consumption data
Loss of data availability

Reputation
Loss of customers

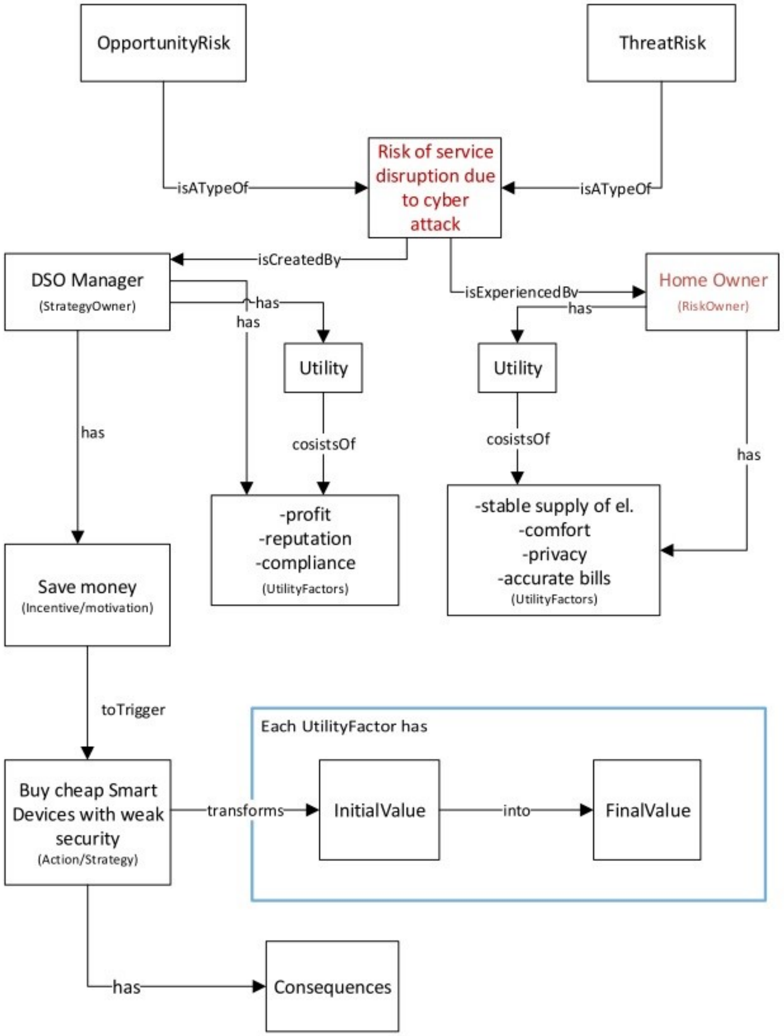
Unreliable service provision

Change provider

Telecommunication
providers

Home Owner (customer)

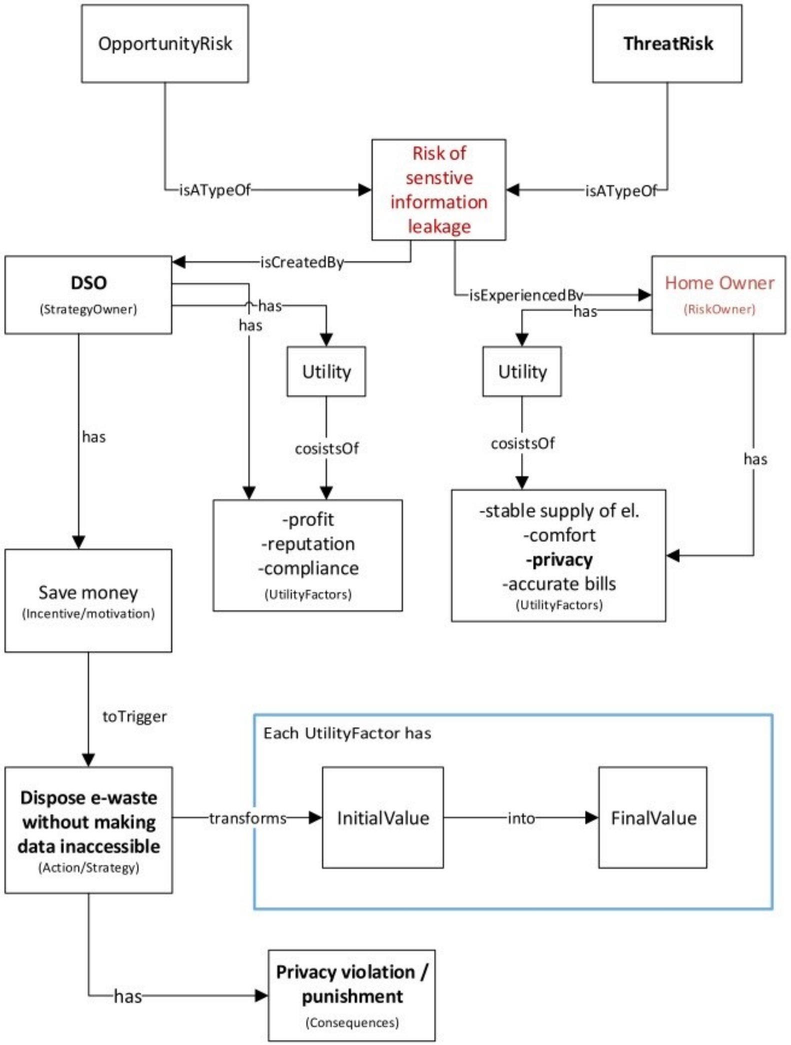
Scenario 3. – DSO as Strategy Owner



Scenario where the strategy owner (Head of purchasing department at a DSO) is responsible for the procurement of Smart Devices that will be utilized in the grid. When making his choice he has to consider several vendors, that vary in their offers in terms of the security, price and capabilities of the devices.

Is he tempted to choose the cheaper ones that come with weaker security measures, therefore leaving customers more vulnerable
to cyber-attacks?

Scenario 4. – DSO as Strategy Owner



Storage of sensitive information about customers and the handling of electronic waste (i.e. discarded devices with sensitive information).

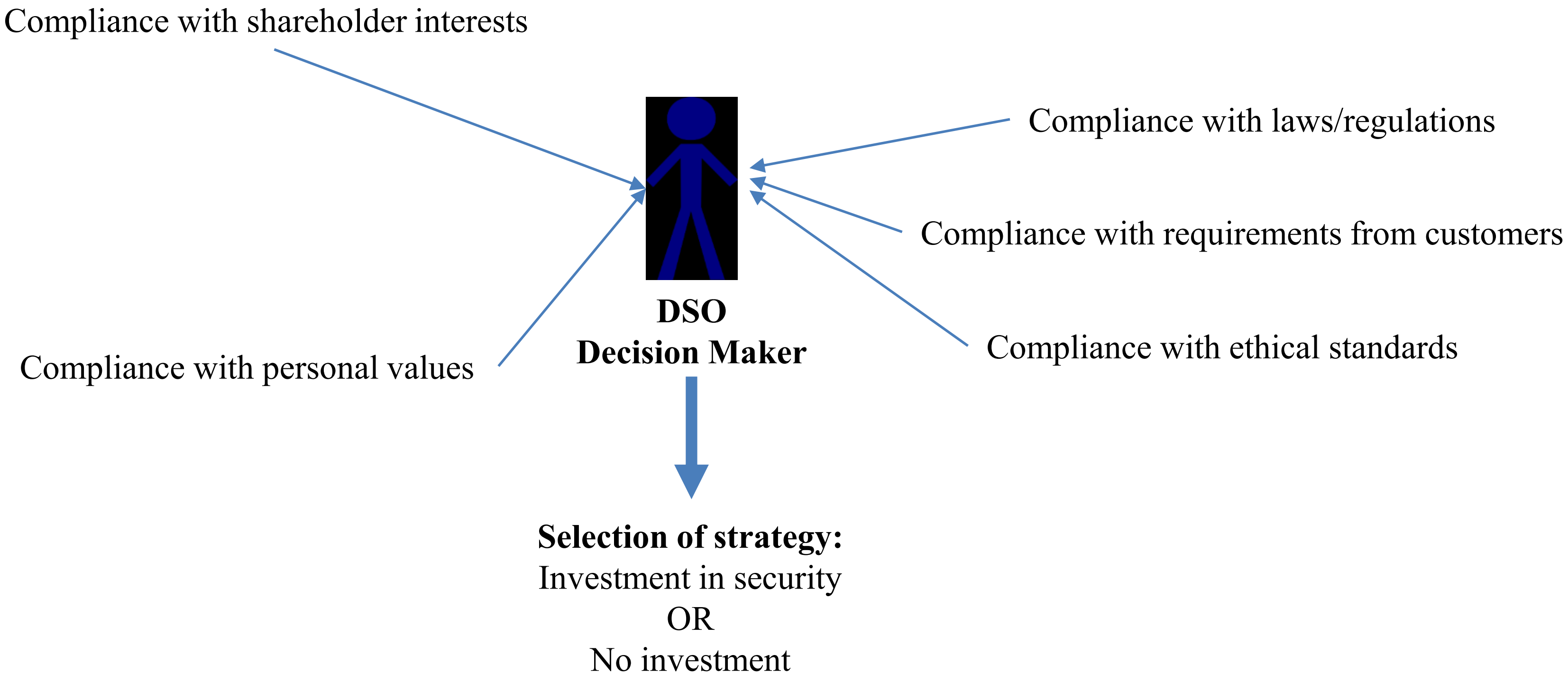
What are the existing practices for handling e-waste?

Risk owner: DSO/Customers
Strategy owner: Data Protection Authority/DSO

Strategies:
- Establish plans that protect privacy after equipment is discarded
- Discard devices without necessary care

Proposed Master thesis topic

Aspects of compliance
DSO as Strategy Owner



Compliance with shareholder interests

Compliance with laws/regulations

Compliance with requirements from customers

Compliance with ethical standards

Compliance with personal values

DSO
Decision Maker

Selection of strategy:
Investment in security
OR
No investment

Perspectives on compliance

Compliance with authorities

- Beside Audits and Penalties for non-compliance
- Norms
- Perceived fairness of the tax system
- Trust in government

Compliance with moral vs social norms

- Public observability of choices results in more equal allocations in dictator game

Compliance in relation to peer behavior

- Providing Performance Indicators (comparing one's achievement to others) increases non-compliance when others are highly non-compliant
- Competitive environments decrease compliance

Compliance with ethical standards

- Framing effect on ethical decision making: - different ethical behaviors under *gain vs loss frames*
- More unethical behavior (gathering insider information to trick competitor, lying) observed in loss frame than in gain frame

Plans for the time remaining

Paper 7. – Choice prediction

- **Research Question**: To what extent is the proposed framework able to predict actual choices? This paper aims at validating the proposed method by presenting participants with choice dilemmas.

- Using input the taxonomy of situations to generate dilemmas, which will be used to assess how well personality and situational features can be combined to predict choices.

Paper 8. – SGAM Human layer

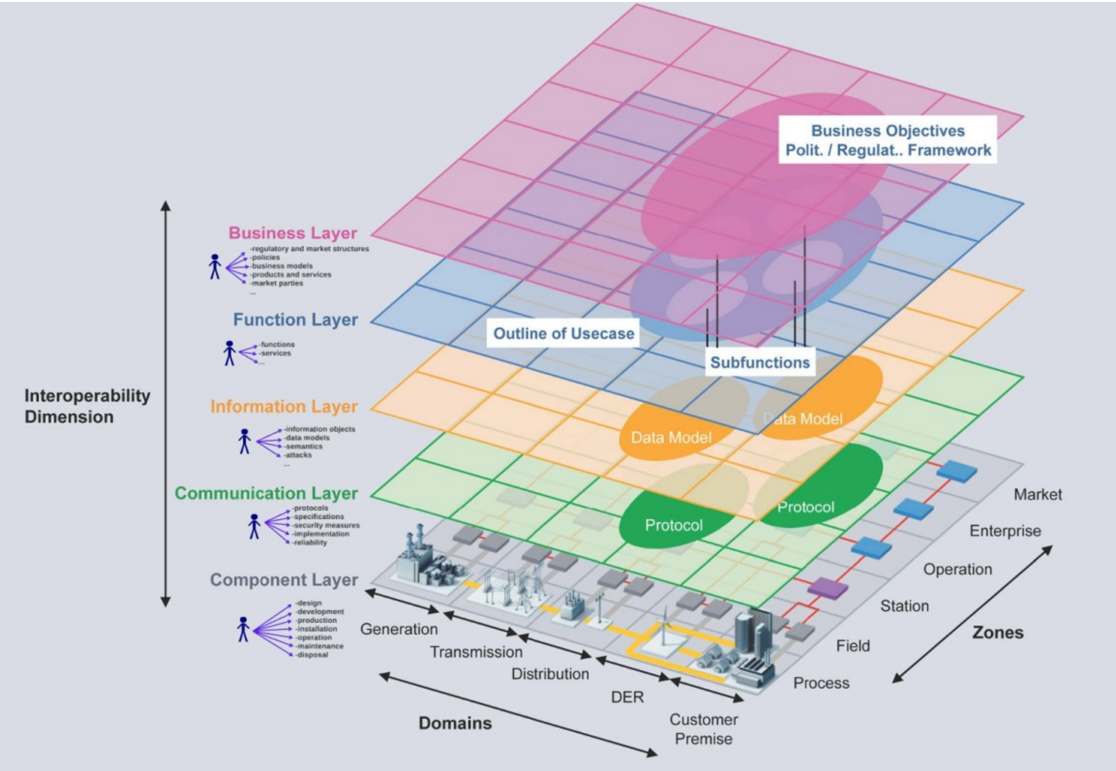
Enable a CIRA-type of risk analysis for Smart Grid scenarios

Need for:
- representing human
actors within the system

Facilitate identification of
 Risk Owners
 Strategy Owners
Define interdependencies
between stakeholders

Implement the model we
used to represent stakeholders

Potential venue for
cooperation


Business Objectives
Polit. / Regulat.. Framework
Outline of Usecase
Subfunctions
Data Model
Data Model
Protocol
Protocol
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
Generation
Transmission
Distribution
DER
Customer
Premise
Domains
Market
Enterprise
Operation
Station
Field
Process
Zones