Security for smart Electricity GRIDs

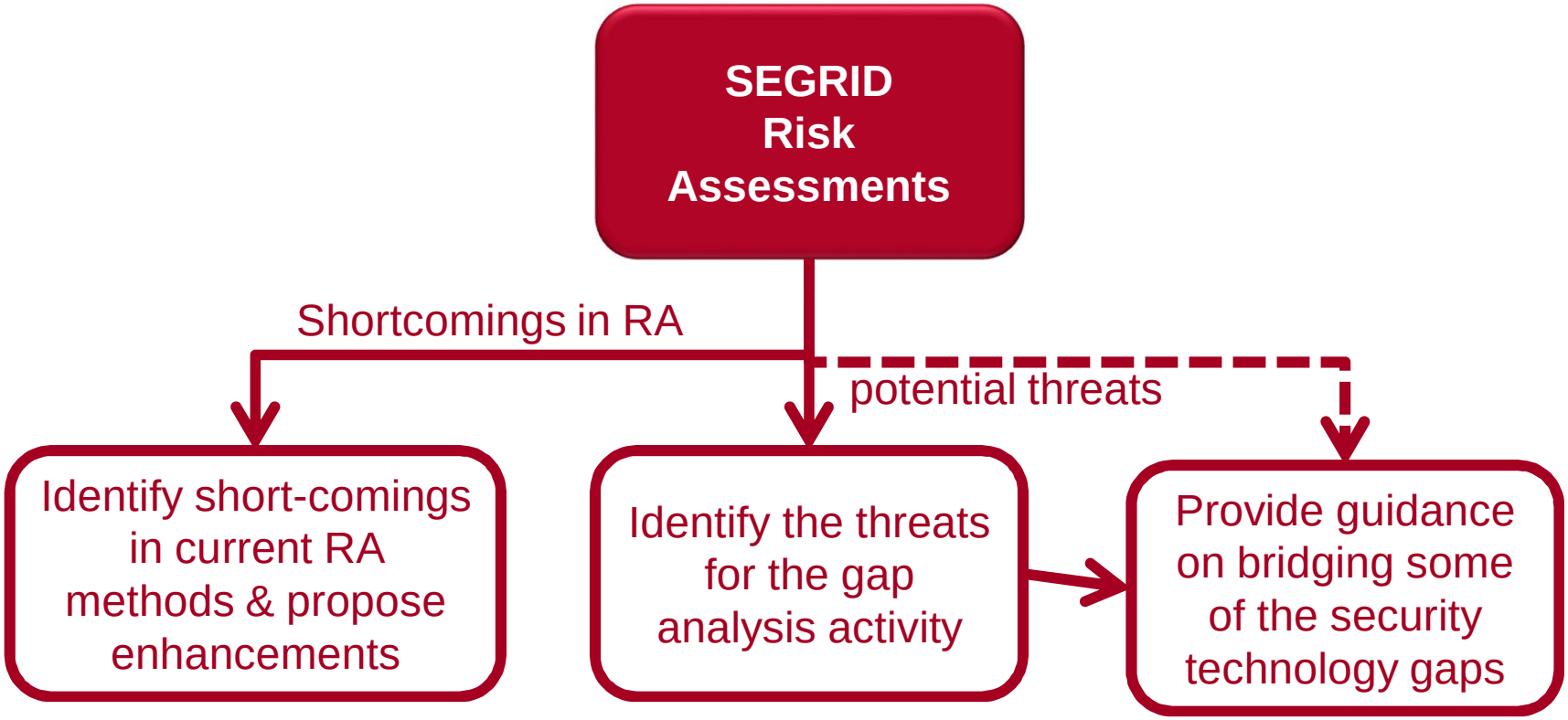
SEGRID Smart Risk Assessment

Judith E. Y. Rossebø

14th November, 2016

SEGRID has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

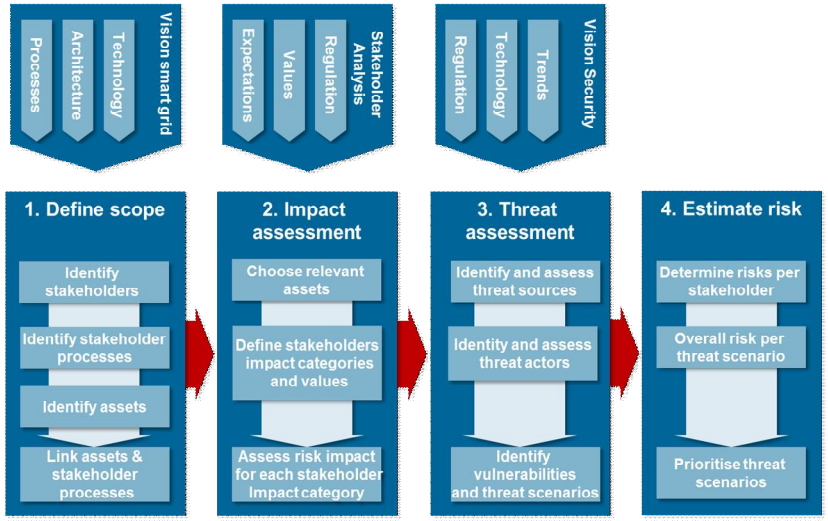
Objective


SEGRID
Risk
Assessments
Shortcomings in RA
potential threats
Identify short-comings in current RA methods & propose enhancements
Identify the threats for the gap analysis activity
Provide guidance on bridging some of the security technology gaps

Applying and enhancing risk assessment

Segrid approach

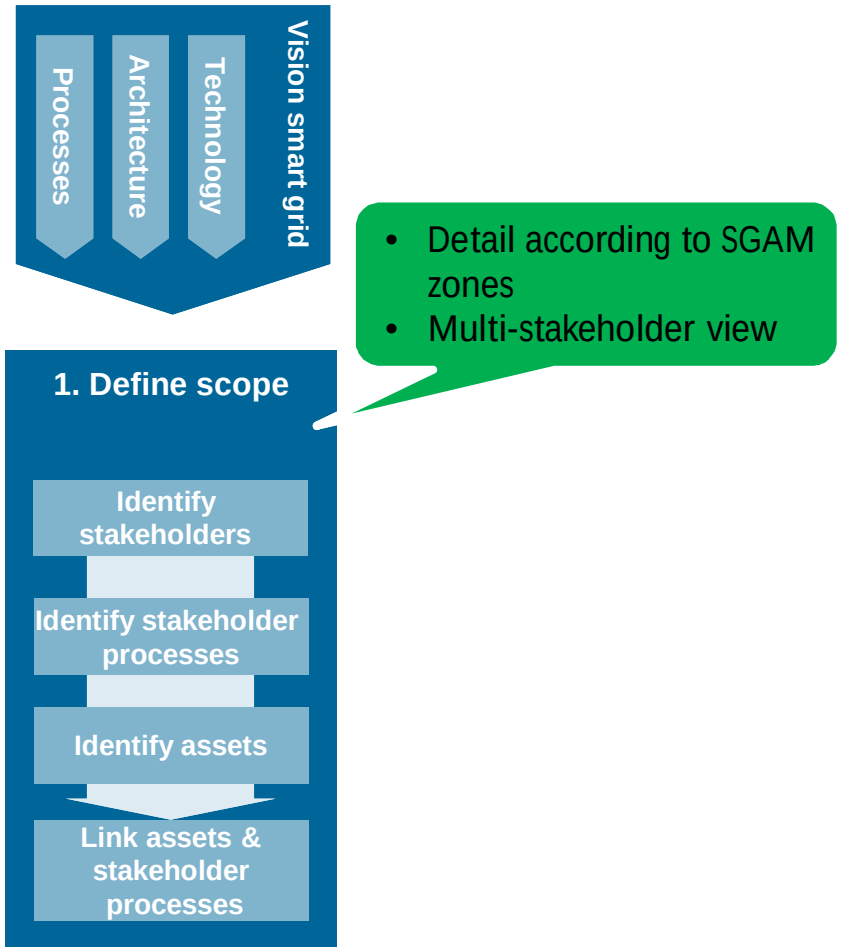
- Risk management
  - Identify, analyse, evaluate and treat risks



- SEGRID four step risk assessment approach
  - Based on HMG IA Standard No. 1 (IS1)
  - Enhanced by adding a multi stakeholder view and using the ETSI TVRA
  - Applied to a selection of SEGRID use cases

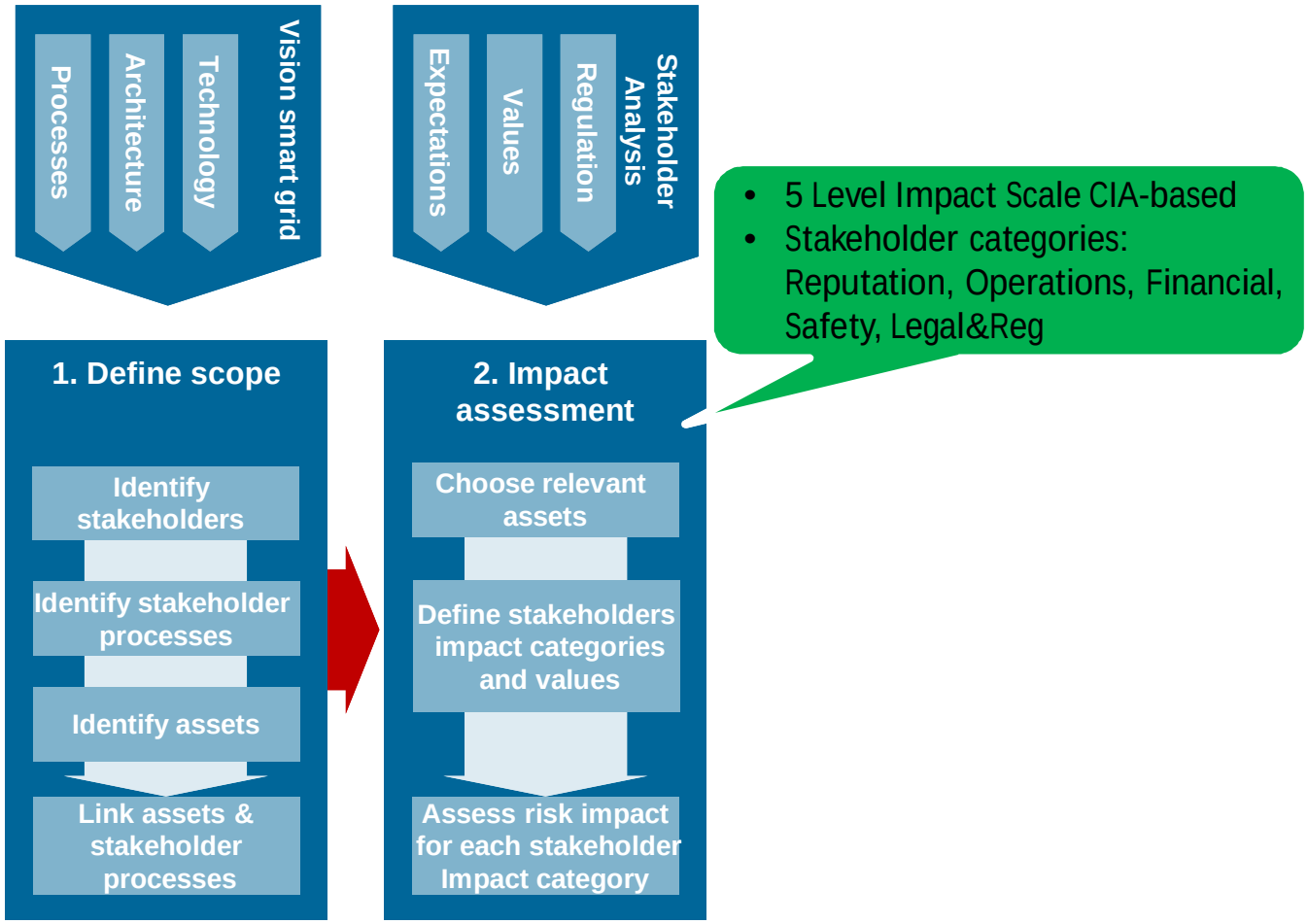
Applying and enhancing risk assessment

Steps in SEGRID Approach to Risk Assessment



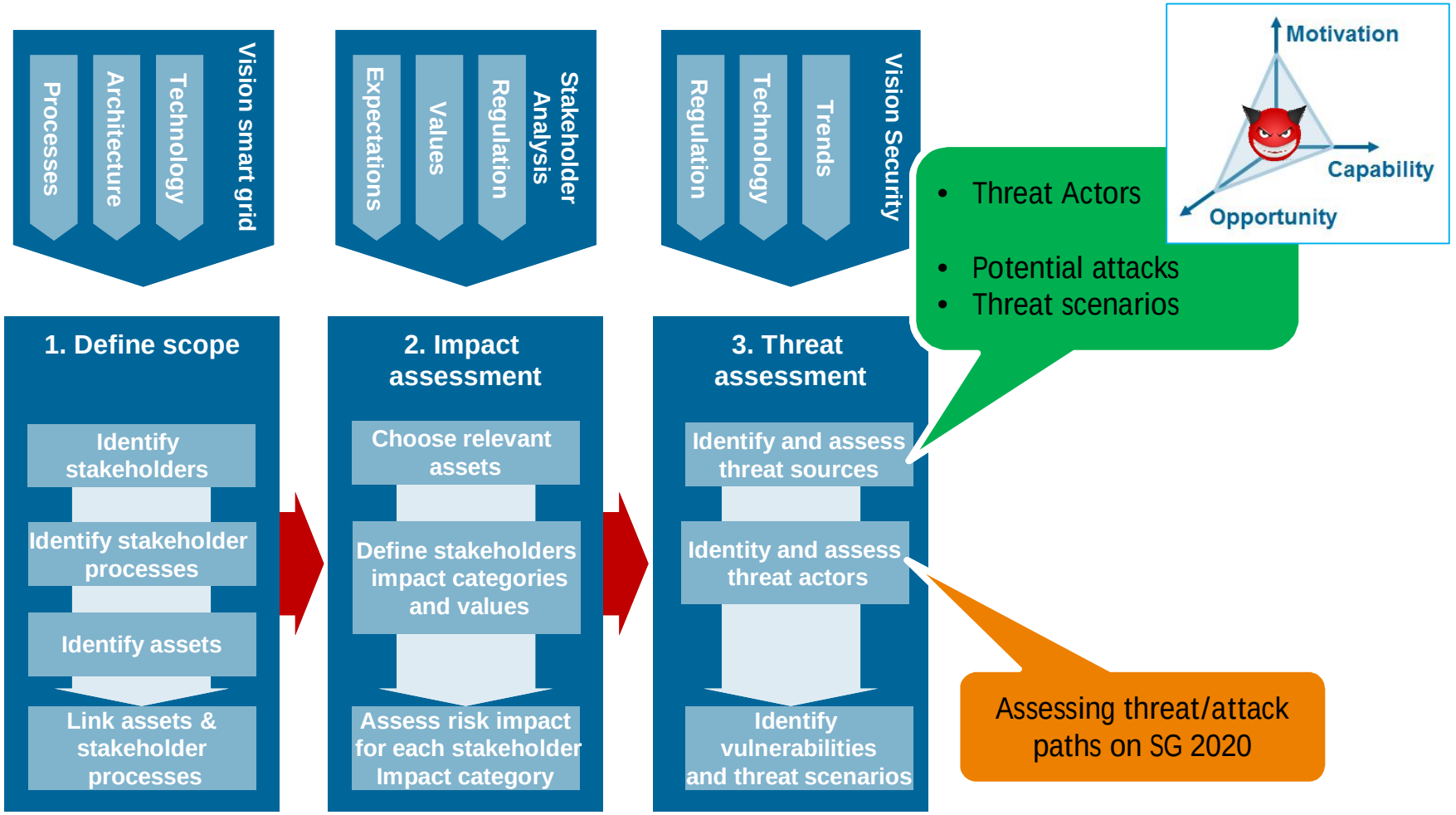
Applying and enhancing risk assessment

Steps in SEGRID Approach to Risk Assessment



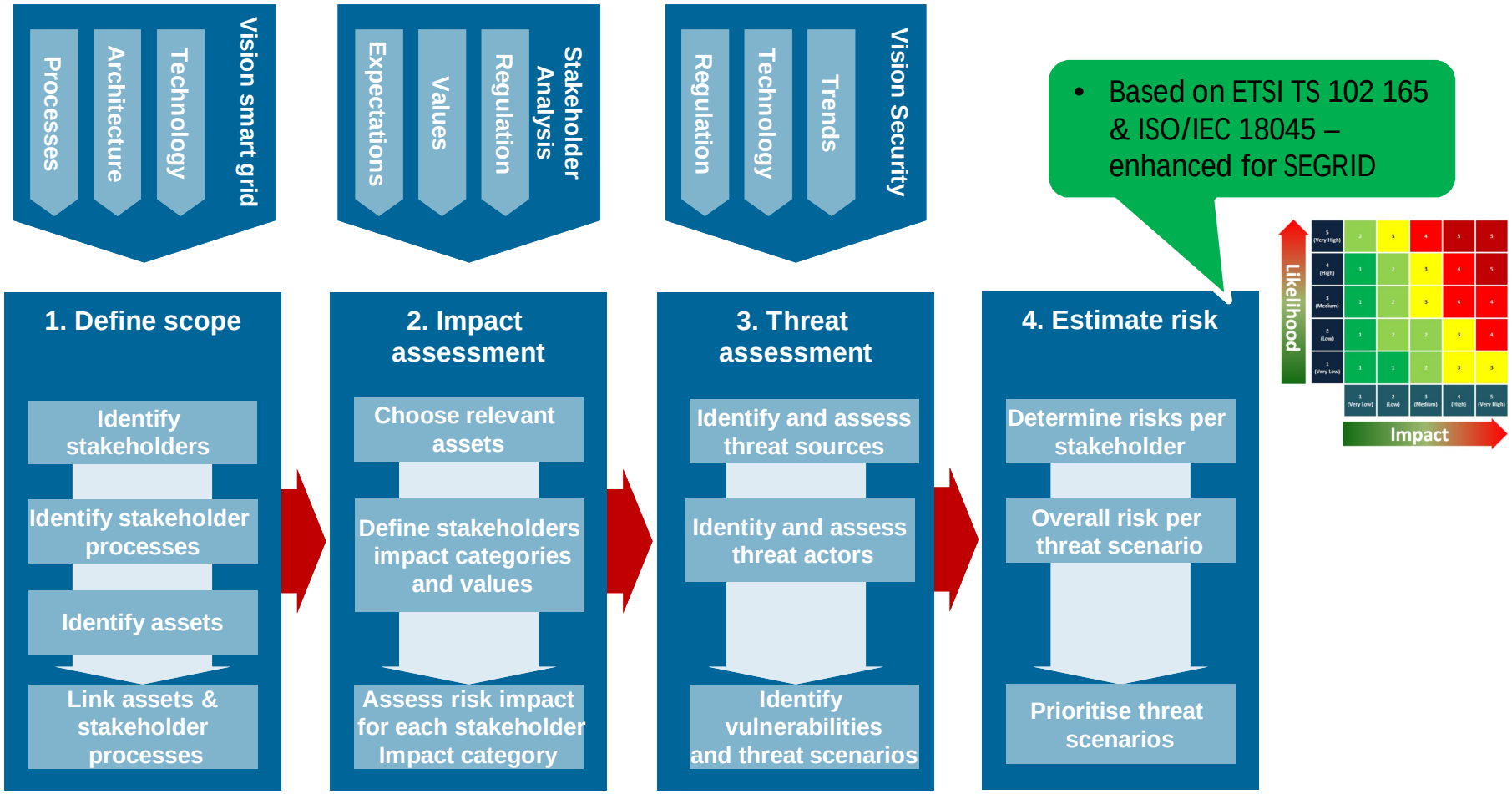
Applying and enhancing risk assessment

Steps in SEGRID Approach to Risk Assessment



Applying and enhancing risk assessment

Steps in SEGRID Approach to Risk Assessment

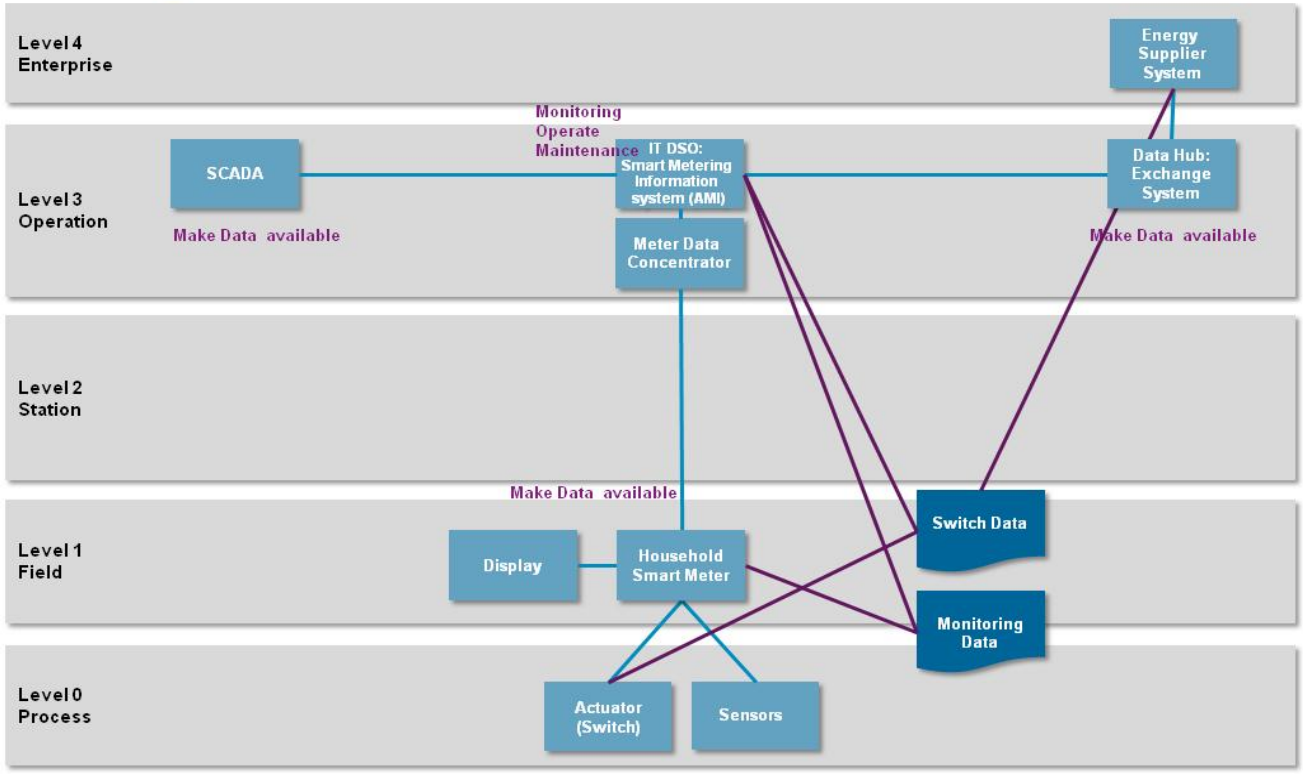


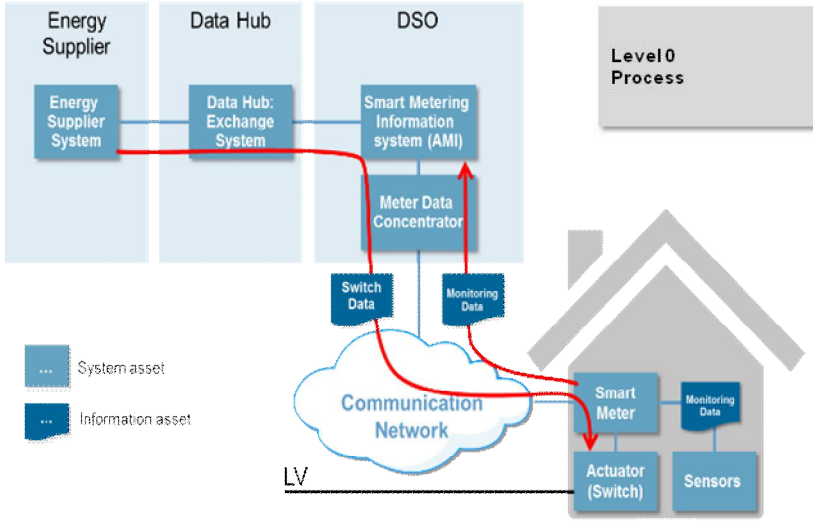
Applying RA to SEGRID use case: Remote power switching

Step 1: Scope of the Risk Assessment

- Use case scope
  - Identify
    - Stakeholders and assets
  - Link stakeholder processes & assets
  - Detailed using SGAM zones

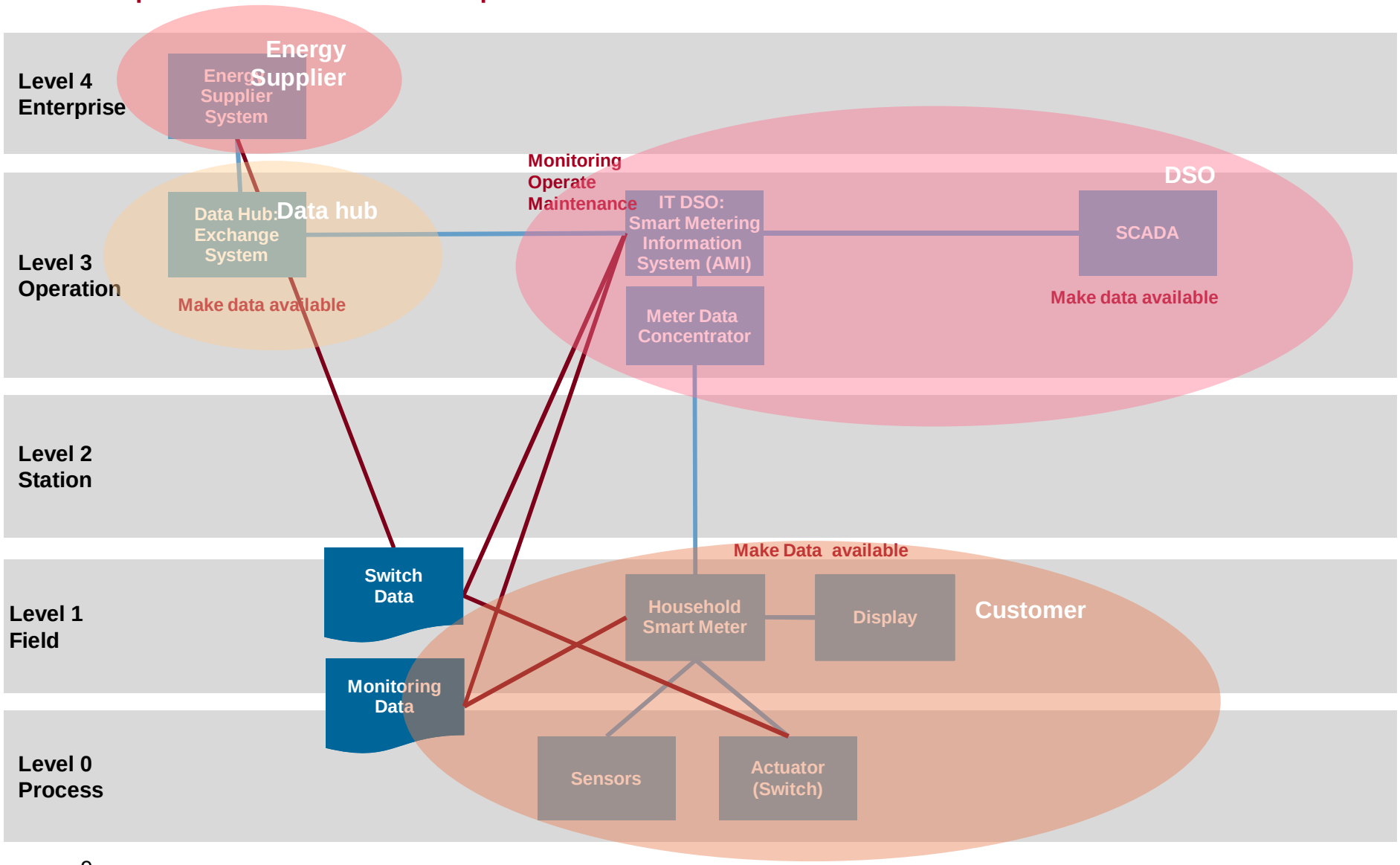
Use Case : Remote power switching





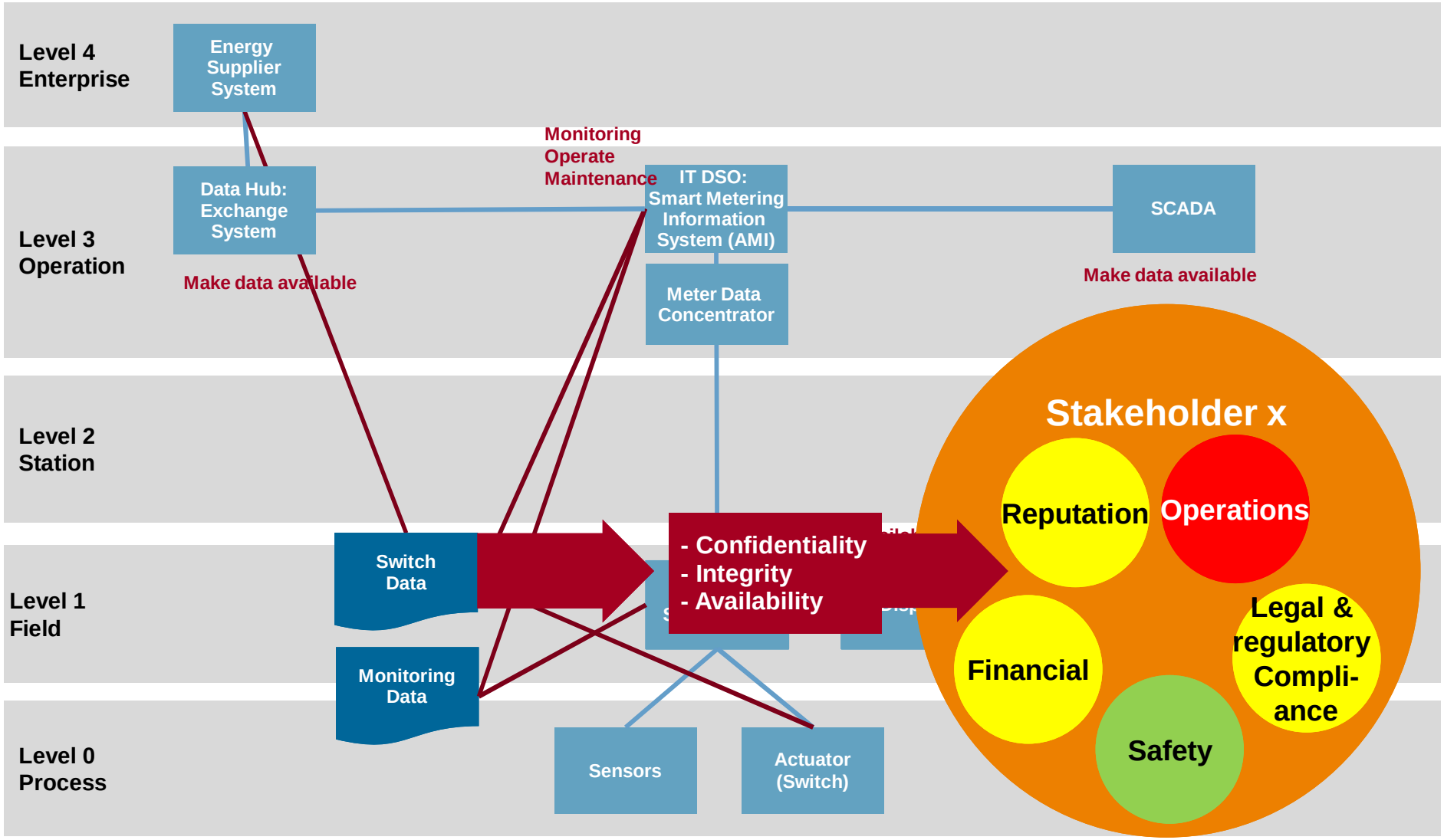
Applying RA to SEGRID use case: Remote power switching

Step 2: Stakeholder Impact Assessment



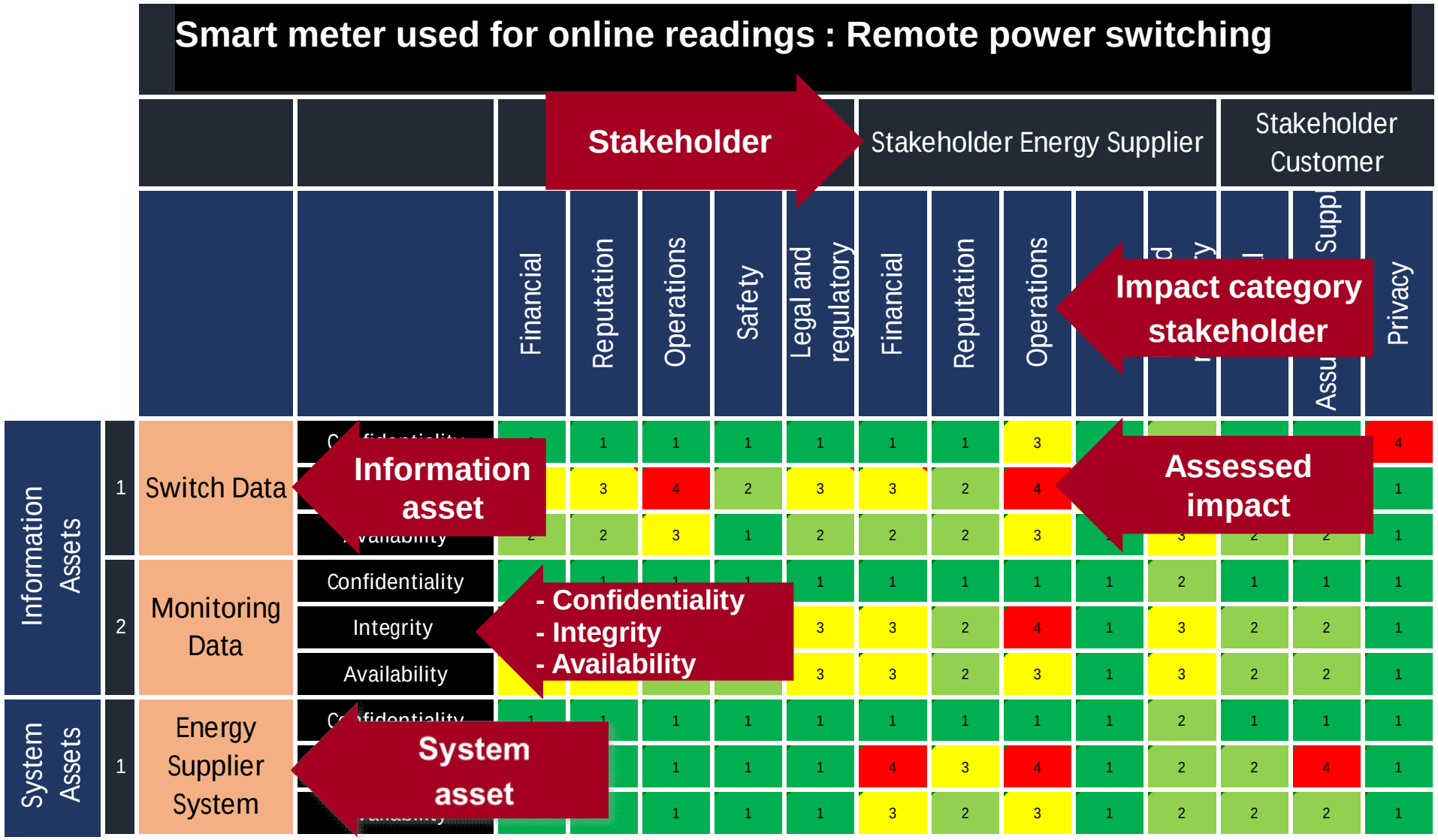
Applying RA to SEGRID use case: Remote power switching

Step 2: Stakeholder Impact Assessment



Applying RA to SEGRID use case: Remote power switching

Step 2: Stakeholder Impact Assessment



But how about Societal Impact?

What kinds of threats have critical impact on society?

Example: Ukraine blackout

- 225,000 Customers: experienced loss of power on Dec 23rd, 2015 (for 1 to 6 hours)

First known hacker-caused power outage signals troubling escalation

Highly destructive malware creates "destructive events" at 3 Ukrainian substations.

by Dan Goodin - Jan 4, 2016 9:36pm CET

Share Tweet Email 112

Krzysztof Lasoń

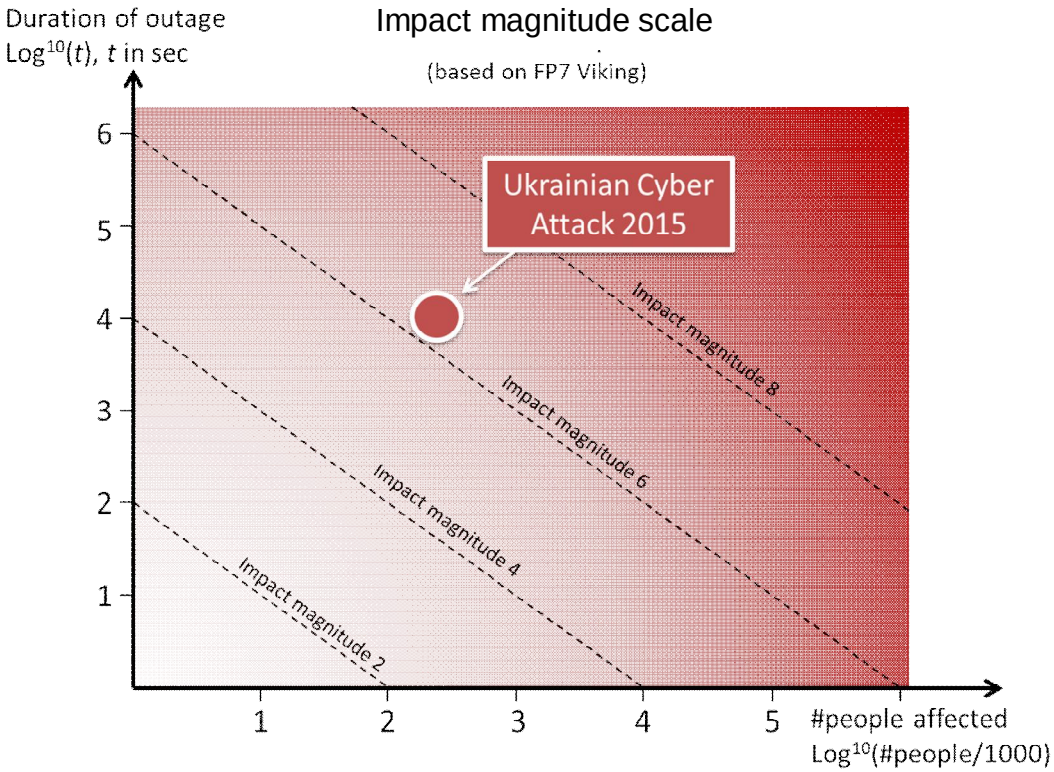
Highly destructive malware that infected at least three regional power authorities in Ukraine led to a power failure that left hundreds of thousands of homes without electricity last week, researchers said.

But how about Societal Impact?

What kinds of threats have critical impact on society?

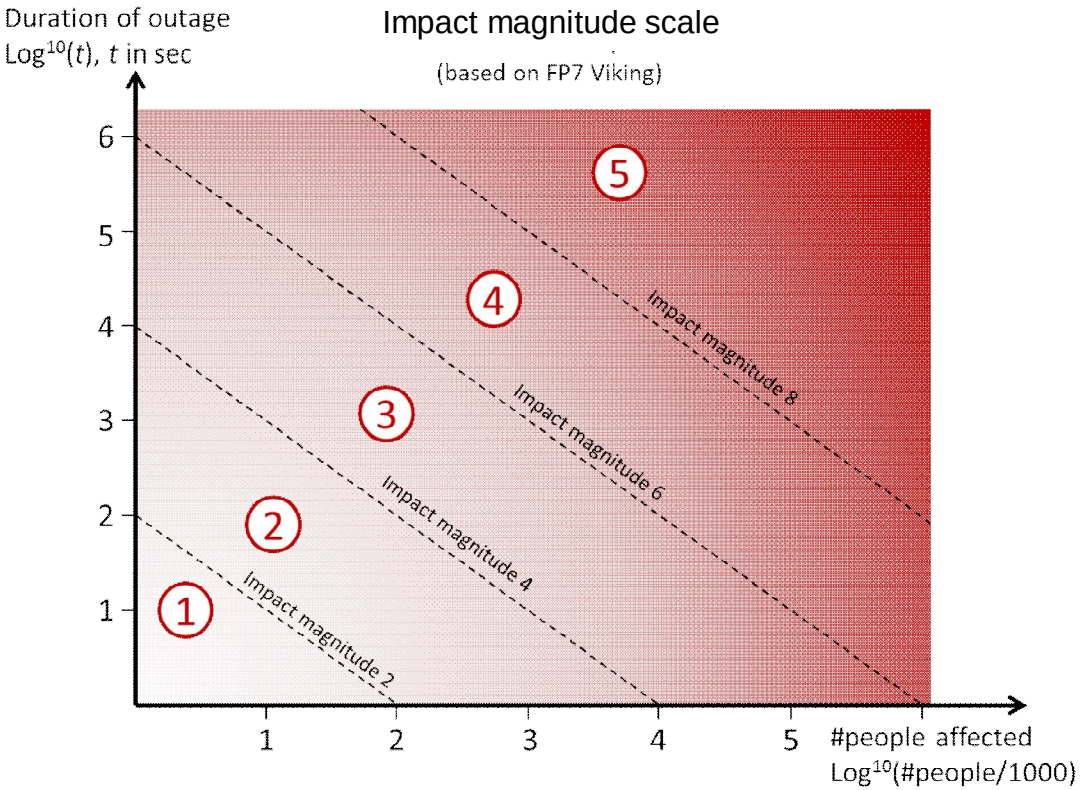
Example: Ukraine blackout

- 225,000 Customers experienced loss of power on Dec 23rd, 2015 (for 1 to 6 hours)



SEGRID adopted the approach from FP7 project Viking to plot power outages on Social Impact Magnitude scale.

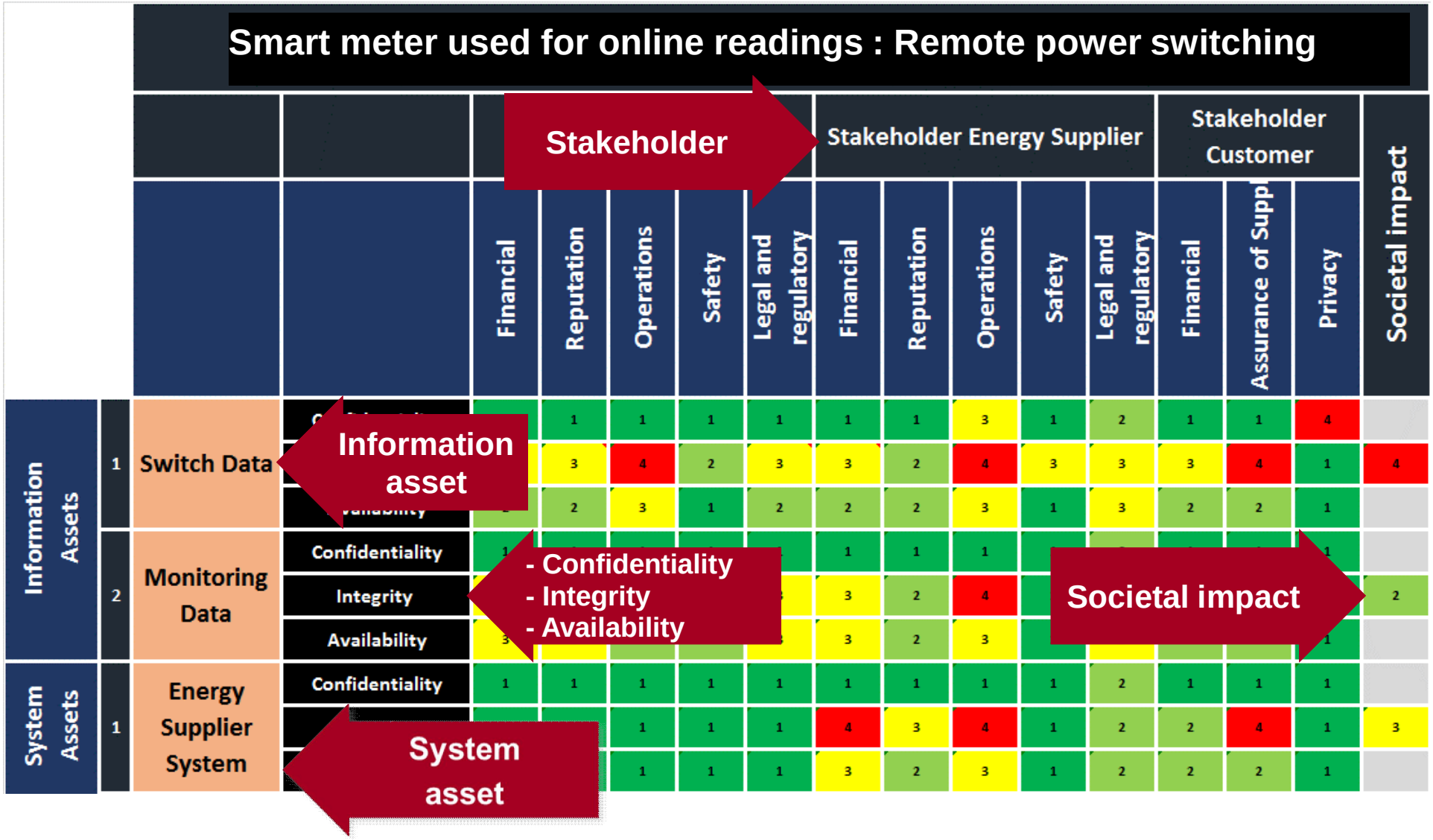
SEGRID Societal Impact Scale



	5 - Very high	4 - High	3 - Medium	2 - Low	1 - Very low
Societal impact	Electricity blackout of Impact magniture >8 - More than 5 million people affected - Duration of more than 12 hours	Electricity blackout of Impact magniture between 6 and 8 - Typical 500000 people affected - Typical duration 4 hours	Electricity blackout of Impact magniture between 6 and 4 - Typical 20000 people affected - Typical duration 2 hours	Electricity blackout of Impact magniture 2 and 4 - Typical 1000 people affected - Duration typical 30 minutes	Electricity blackout of Impact magnitude <2 - Typical 1000 people affected - Duration less than 1 minute

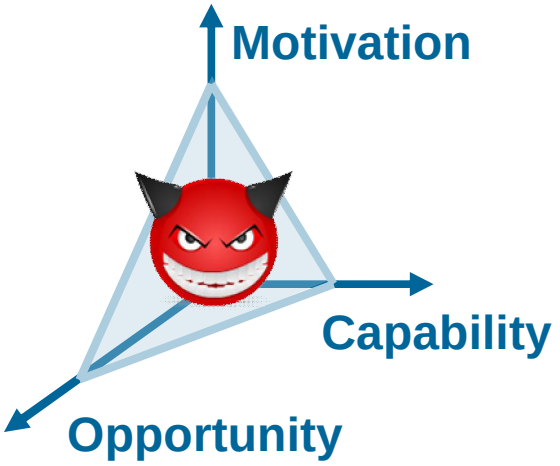
Applying RA to SEGRID use case: Remote power switching

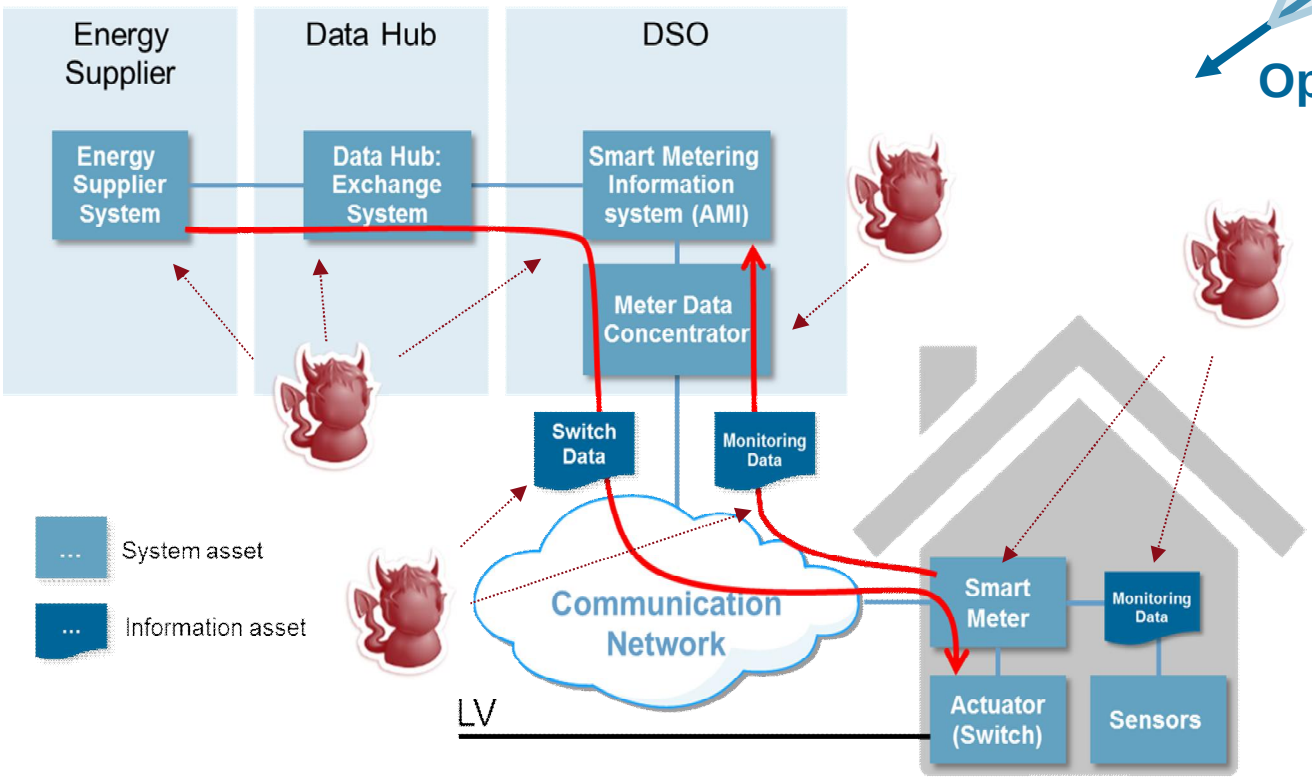
Step 2: Stakeholder Impact Assessment



Step 3: Threat and Vulnerability Assessment

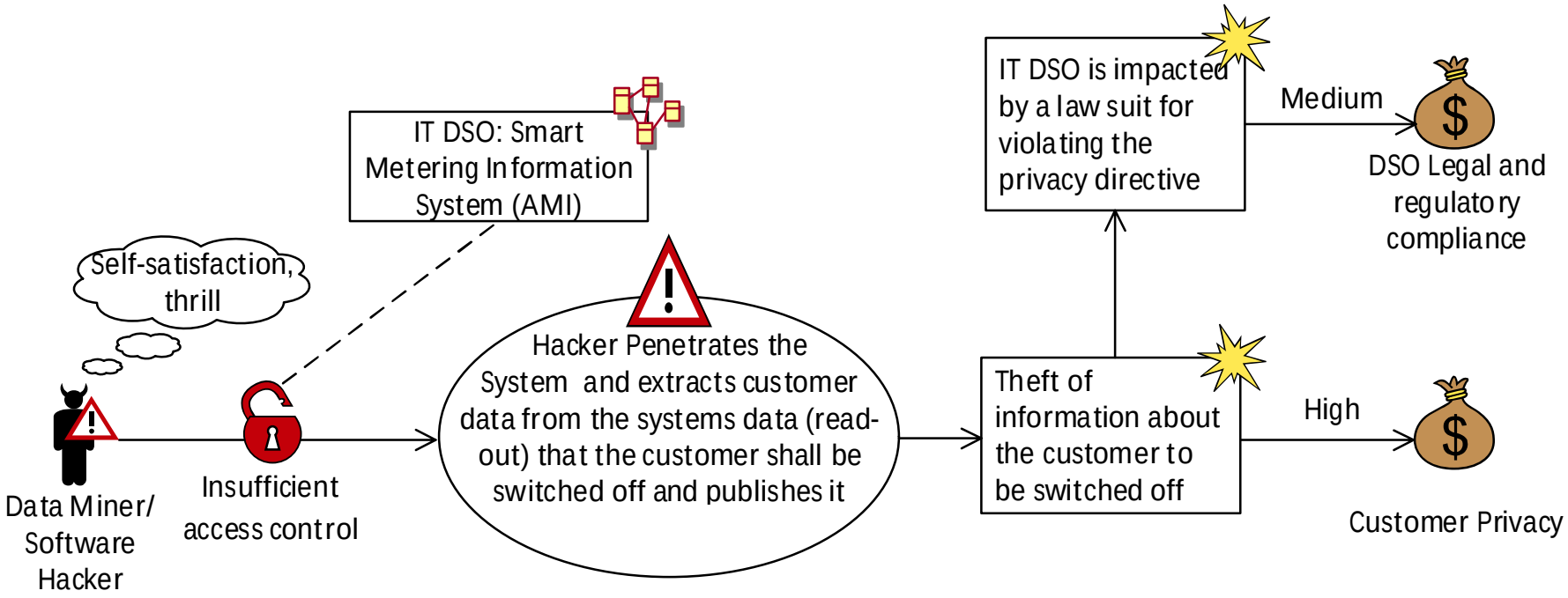
- In the scope of the Use Case
  - Identify
    - Threat Actors
    - Potential attacks
    - Threat scenarios





Step 3: Threat and Vulnerability Assessment

- Adopted CORAS threat scenario diagams to describe threat scenarios

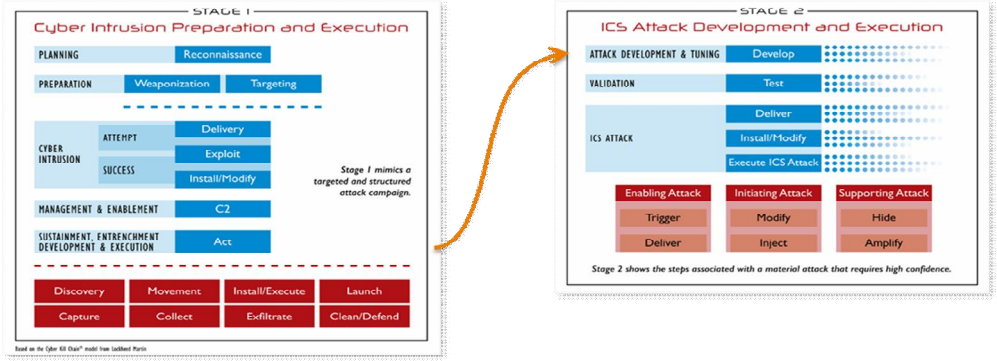


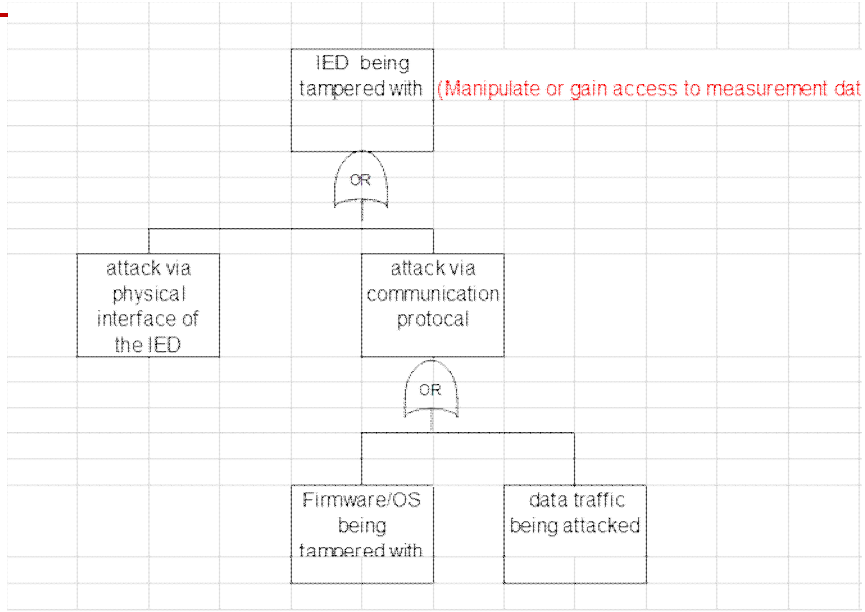
Step 3: Threat and Vulnerability Assessment

Aids to support identification of threat scenario's and attacks

- *Threat lists / attack libraries*

  e.g. Threat List from 1st Expert Group, CAPEC & ATT&CK from MITRE, etc.
- *CySeMoL*
- *Attack Trees*
- *ICS Cyber Kill Chain (SANS)*

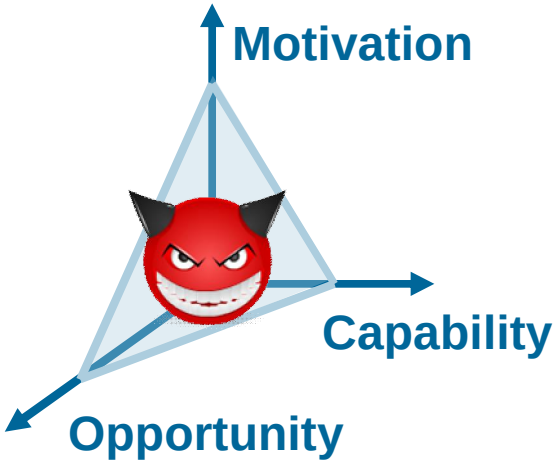




Step 4: Risk Estimation

Based on ETSI TS 102 165 & ISO/IEC 18045 – enhanced for SEGRID

- Likelihood estimation
  - With TVRA we score what an attacker has to be able to do in terms of Time, Expertise, Knowledge, Opportunity, and Equipment
    - higher score means that the attacker has to have a higher attack potential
    - Scores are used as a metric for likelihood



- Impact estimation
  - Intensity of the attack is a factor of the Impact

What about Motivation?

Threat Group	Threat Description	Attack						Impact	Risk
		Factor	Notes	Range	Value	Potential	Likelihood		
Manipulate, Integrity	Vulnerability: Datahub Exchange system has software vulnerabilities, accessible Scenario: Attacker manages to penetrate system and sends switch off commands to very many customers. The attack can be carried out by exploiting a vulnerability to install a malicious process that tries to influence and/or	Time	attack requires some planning	<= 3 months	13	Beyond High	Very Unlikely	Very high	Major
		Expertise	expert in these systems (insider, state sp	Expert	5				
		Knowledge	knowledge of AMI internals is not publicly	Restricted	1				
		Opportunity	remote access, inside access	Difficult	12				
		Equipment	PC	Standard	0				
		Asset Impact	Very many customers lose power, Energy	High	4				
		Intensity	Attacking large number of customers at o	High intensity	2				

Opportunity

Capability

(Risk = likelihood X impact)

Step 4: Risk Estimation

What about motivation?

- Likelihood depends also on level of **Motivation** & **Capability** of the attacker

- **Examples**: **Stuxnet**, the **Ukrainian power outage** are real examples that demonstrate that threat actor capability and motivation influence likelihood

What about motivation?

Threat Group	Threat Description	Attack						Impact	Risk
		Factor	Notes	Range	Value	Potential	Likelihood		
Manipulate, Integrity	Vulnerability: Datahub Exchange system has software vulnerabilities, accessible Scenario: Attacker manages to penetrate system and sends switch off commands to very many customers. The attack can be carried out by exploiting a vulnerability to install a malicious process that tries to influence and/or	Time	attack requires some planning	<= 3 months	13	Beyond High	Very Unlikely	Very high	Major
		Expertise	expert in these systems (insider, state sp	Expert	5				
		Knowledge	knowledge of AMI internals is not publicly	Restricted	1				
		Opportunity	remote access, inside access	Difficult	12				
		Equipment	PC	Standard	0				
		Asset Impact	Very many customers lose power, Energy	High	4				
		Intensity	Attacking large number of customers at o	High intensity	2				

Opportunity

Capability

(Risk = likelihood X impact)

Including threat actor capability and motivation

Starting point: Likelihood Estimation in the ETSI TVRA

Based on the CC CEM (ISO/IEC 18045)

Factor ∑	Attack Potential	Likelihood
0 to 9	Basic	Very likely
10 to 13	Enhanced Basic	Likely
14 to 19	Moderate	Possible
20 to 24	High	Unlikely
>24	Beyond high	Very Unlikely

Attack Scenario →

Factor	
Time	4
Expertise	6
Knowledge	3
Opportunity	4
Equipment	3
∑	**20**

→ Required **Attack Potential** → **Likelihood** of attack

Depends also on level of **Motivation** & **Capability** of the attacker

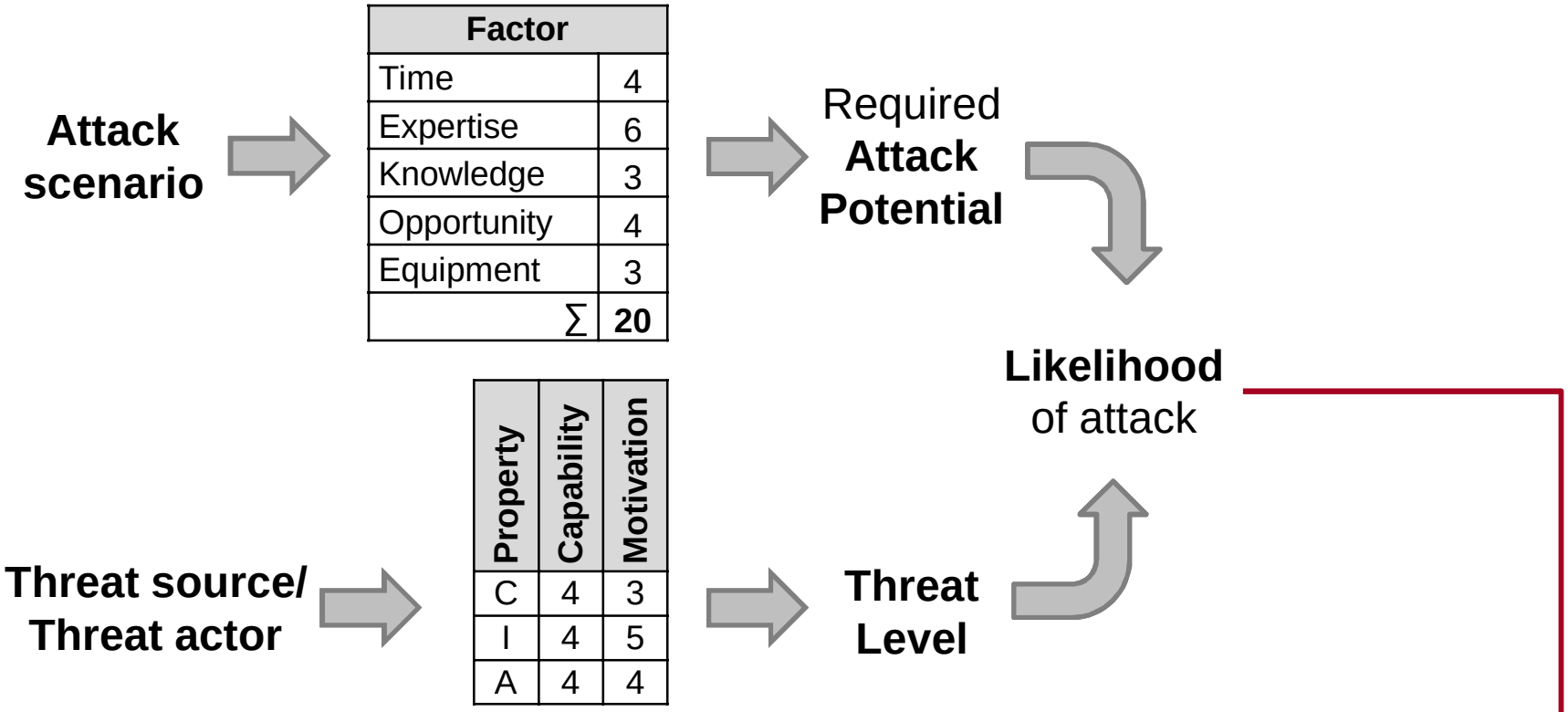
Including threat actor capability and motivation

Threat actor analysis (based on IS1)

Capability of the threat source/actor is combined with motivation

Threat Actor ID	Threat Source name	Description (and rationale)	property	Capability	Motivation	Threat level	Source(of information about threat source)	Threat actors (employed)
Ex 1	Organised Crime Group	The aim is to gain financially from causing outages	C	4	3	Severe	Business Blackout report	hackers
			I	4	5	Critical	Business Blackout report	hackers
			A	4	4	Severe	Business Blackout report	hackers
Ex 2	Hacktivists	libertarianism, anti-establishment ideology, freedom of information and anti-surveillance, environmentalism, and anti-capitalism	C	2	4	Low	media	N/A
			I	3	4	Moderate	media	N/A
			A	3	4	Moderate	media	N/A
Ex 3	Unidentified group	motivated to cause significant disruption of an entire region in a coordinated cyber-attack	C	3	3	Moderate	ICS-CERT (attack on Ukrainian DSOs)	group of hackers/ programmers
			I	5	5	Critical	CS-CERT (attack on Ukrainian DSOs)	group of hackers/programmers
			A	5	5	Critical	CS-CERT (attack on Ukrainian DSOs)	group of hackers/ programmers

Likelihood Estimation Enhanced

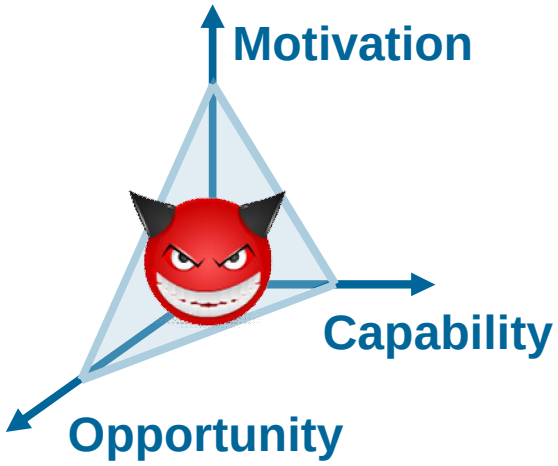


Likehood of attack		Threat Level				
		Negligible	Low	Moderate	Severe	Critical
Attack Potential	Basic	Possible	Likely	Very Likely	Very Likely	Very Likely
	Enhanced Basic	Unlikely	Possible	Likely	Very Likely	Very Likely
	Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
	High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
	Beyond high	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

Risk Estimation enhanced

Based on ETSI TS 102 165 & ISO/IEC 18045 – enhanced for SEGRID

- **Likelihood** estimation
  - Attack Potential (**Opportunity and Required Capability**) is combined with the
  - Threat level (**Motivation & Capability of the Threat Actor**)
- **Impact** estimation
  - Combines Asset Impact with attack Intensity



Threat Scenario Description	Unwanted Incident/ Event	Attack						Impact	Risk
		Factor	Notes	Range	Value	Potential	Likelihood		
Attackers who, leveraging legitimate credentials obtain access to 3 DSOs, remotely operated breakers to disconnect power. Some further systems are wiped using KillDisk malware at the end of the attack. Courruption of Firmware of Serial-to-Ethernet devices at substations. Scheduled power outages to interfere with restoration efforts.	Large number of customers (225,000) lose power, Energy supplier impacted, DSO operations, reputation	Time	attack requires some planning	> 6 months	19	Beyond High (f_1)	Possible (f_2)	Very high (f_3)	Critical (f_4)
		Expertise	expert in these systems	Multiple experts	8				
		Knowledge	knowledge of SCADA, RTUs	Restricted	3				
		Opportunity	remote access, inside access	Moderate	4				
		Equipment	PCs, VPN and ICS client software	Standard	0				
		Threat level	Ref Threat actor analysis	Critical	4				
		Asset Impact	Very many customers lose power, En	High	4				
		Intensity	Attacking 3 DSO many customers	High intensity	2				

Opportunity

Required Capability

Motivation and Capability of the Threat Actor

SEGRID TVRA enhancements

Contribution to a Standardization Body

- ETSI TC Cyber
  - Centre of expertise in the area of Cyber Security
- ETSI TC Cyber adopted a new WI to revise TS 102 165-1 (TVRA) in June
- TNO, ABB submitted a CR based on results of WP2 in September
  - Update of the TVRA Tool to the latest version of the CC CEM
  - Update of the TVRA method and tool with the enhancements to include Threat Actor Capability and Motivation in the Risk Assessment

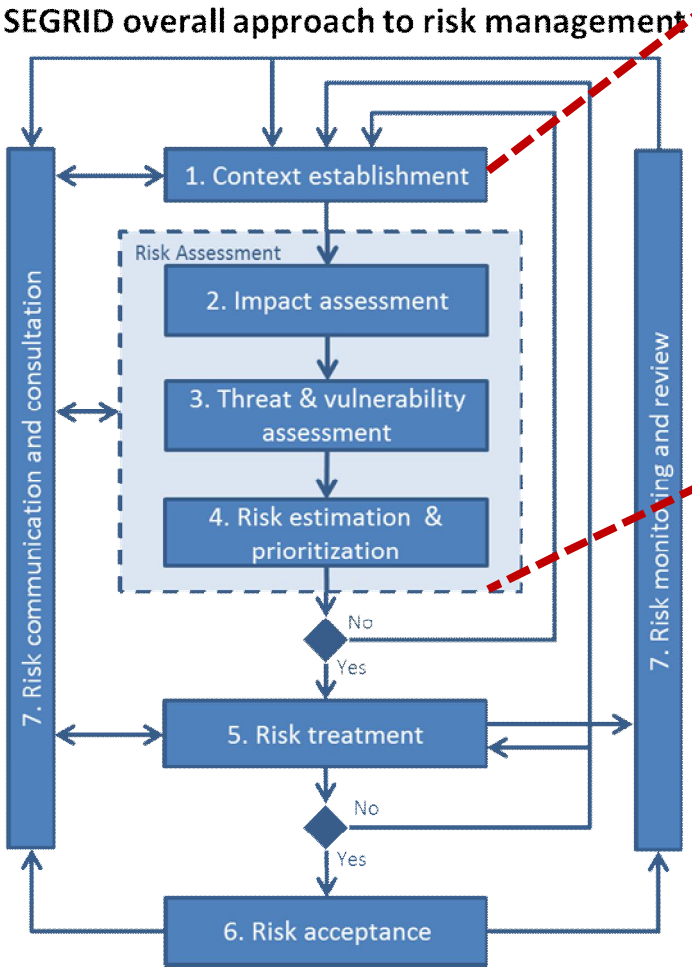
The Contribution was accepted in the next version of the standard. This ensures that the Threat, Vulnerability and Risk Assessment work will be used.

SEGRID Risk Management Methodology

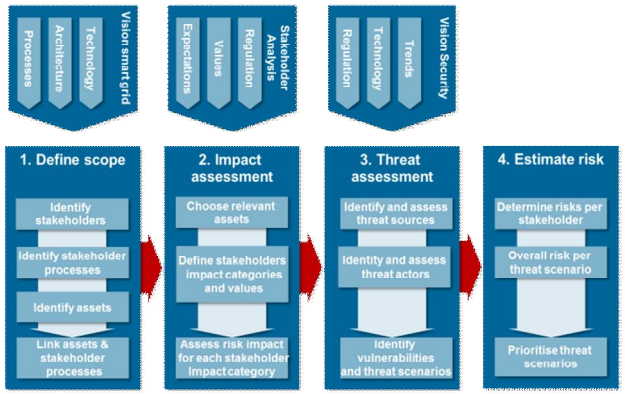
- Extending the 4 step approach to a full risk management approach

The SEGRID Risk Management Methodology

Based on ISO/IEC 27005

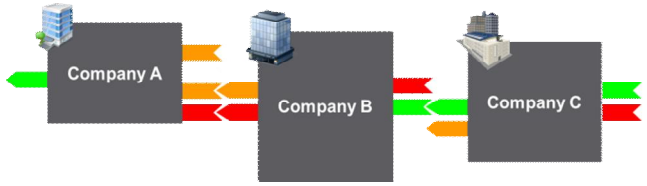


SEGRID Approach to RA



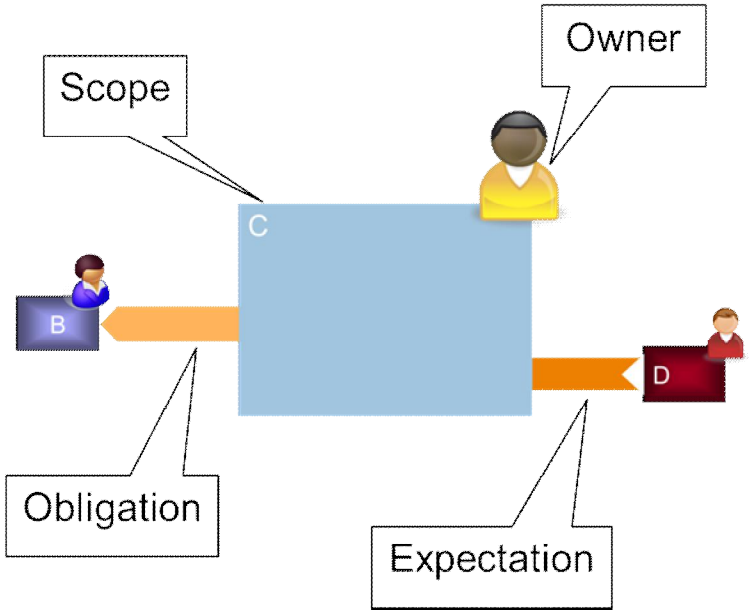
Network Risk Management

Further enhancements to support multi-stakeholder



Network Risk Management approach

Demarcation of responsibility & insight in value chain

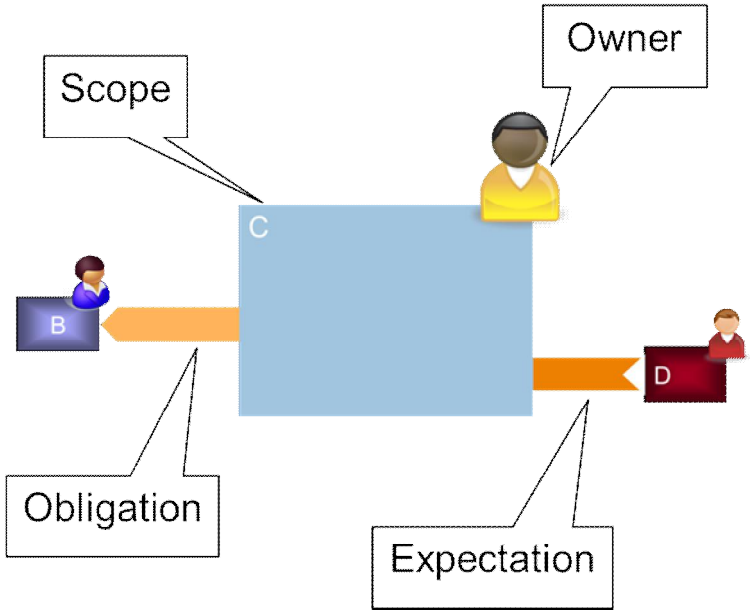


- A **Scope** is a demarcation of responsibility of an **Owner**.
- Each scope has **Obligations** to other scopes.
- Each scope has **Expectations** on other scopes that are needed in order to fulfill its own obligations.

Network Risk Management approach

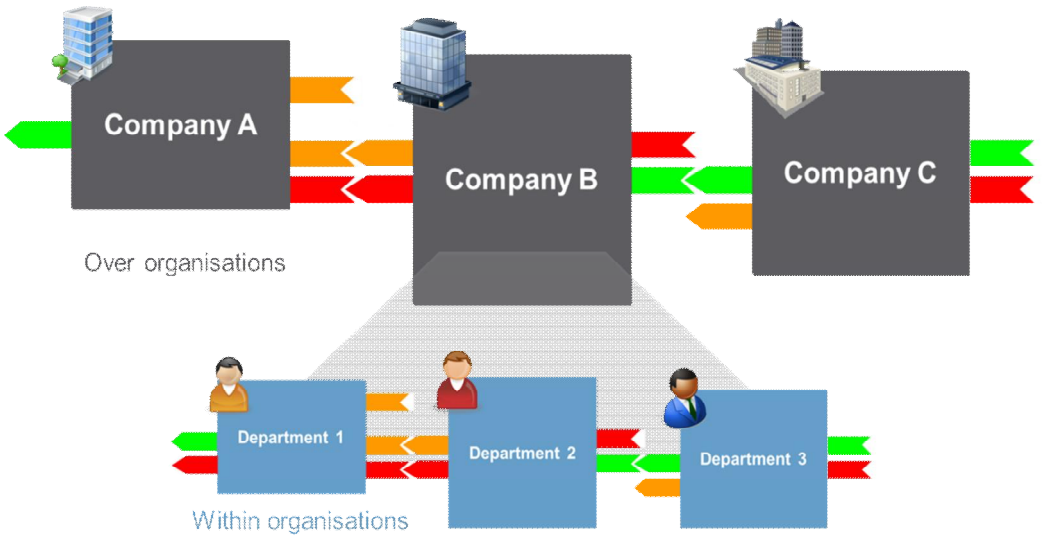
Obligation impact assessment

- Each obligation that is not fulfilled leads to a certain **impact** on the scope owner.



SEGRID Risk Management Methodology

Using the NRM



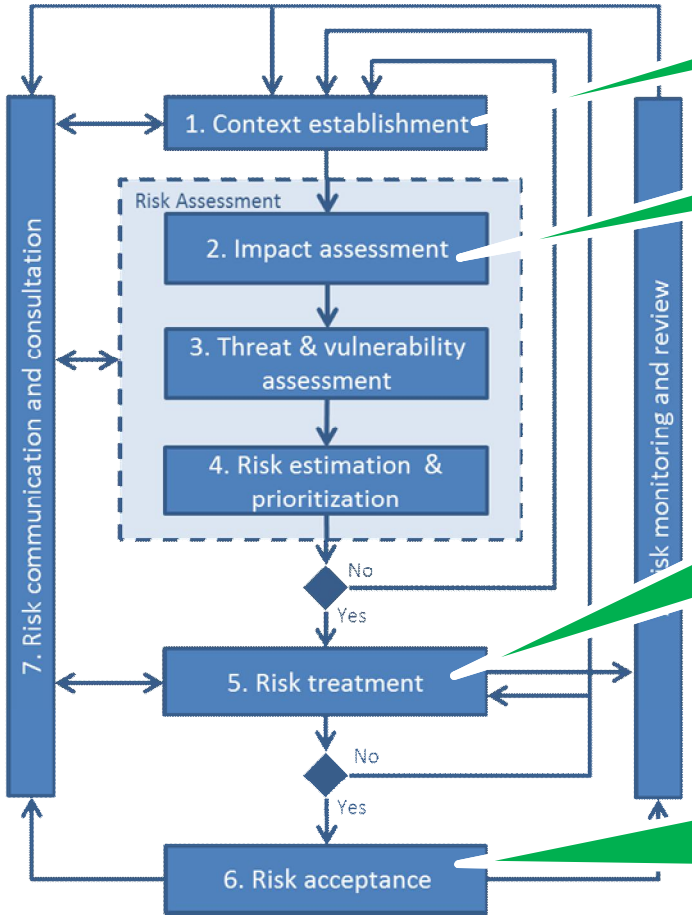
In SEGRID risk management methodology we applied NRM to provide:

- **Clearer demarcation** of the stakeholder scope and responsibilities, which will provide better insight in the value chain.
- Improved **insight in dependencies** between stakeholders, which will improve the quality of the impact assessment.
- Support **assigning responsibilities** in the risk treatments and risk acceptance.

The SEGRID Risk Management Methodology

Based on ISO/IEC 27005

SEGRID overall approach to risk management



- Define NRM scopes, obligations and expectations
- verify if they match between scopes

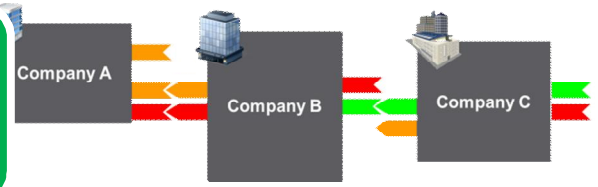
- Assess impact on Obligations in each Scope

- report structured along the Obligations and Expectations

- risk acceptance decision is made, using the ownership of the NRM scope

Network Risk Management

Further enhancements to support multi-stakeholder



Concluding remarks

- Innovation in cyber security for smart grids is needed to stay ahead of the threats

- The SEGRID RA approach builds on state of the art RA methodologies while providing guidance and enhancements for use in smart grids.

- We applied the SEGRID approach to selected use cases
  - § Demonstrating suitability for RA across multiple stakeholders
  - § Identifying the need to include the threat actor analysis in the RA for smart grids

- We have enhanced the SEGRID approach:
  - Including the threat actor motivation and capability in the risk estimation step
  - Inlcuding societal impact
  - Including NRM for a clearer demarcation of the stakeholder scope, and improved insight in dependencies between stakeholders

Questions

Judith E. Y. Rossebø, PhD
Cyber Security Specialist
ABB AS

Phone: +47 22874725
Mobile: +47 41563062
E-mail: judith.rossebo@no.abb.com

Mail: info@segrid.eu
Website: www.segrid.eu
Telephone: +31 8886 67758

Project type: Collaborative project – small or medium scale focused research project
Grant agreement no: 607109
Thematic Priority: FP7-SEC-2013-1
Start date of project: October 1st, 2014
Duration: 36 months
Coordinator: TNO, The Netherlands