Security for smart Electricity GRIDs

An Enhanced Risk Assessment Methodology for Smart Grid – applied to UC2 Sce2

Judith E. Y. Rossebø and Reinder Wolthuis

2nd October, 2017

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

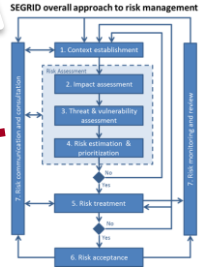
Risk Management & SEGRID Innovations

Risk management

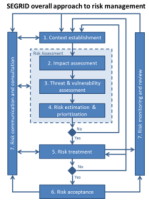
Periodic update

Toward dynamic / real-time risk management

SRMM

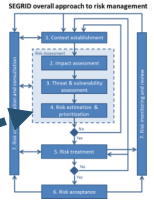


Changes in:
- Threat landscape
- Infrastructure
- Business objectives
- Risk appetite



securiCAD

use



Security Operations

Vulnerability Management, Security Incident Monitoring & Incident Response

automatic model creation & updating

Power Grid Infrastructure

Power Grid Infrastructure

Power Grid Infrastructure

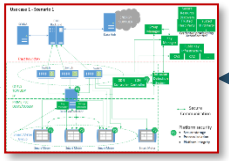
Operations

Development

Risk assessment

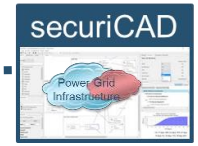
SPADE

Security & Privacy Architecture with *SEGRID security solutions*



check

securiCAD



modelled

integration

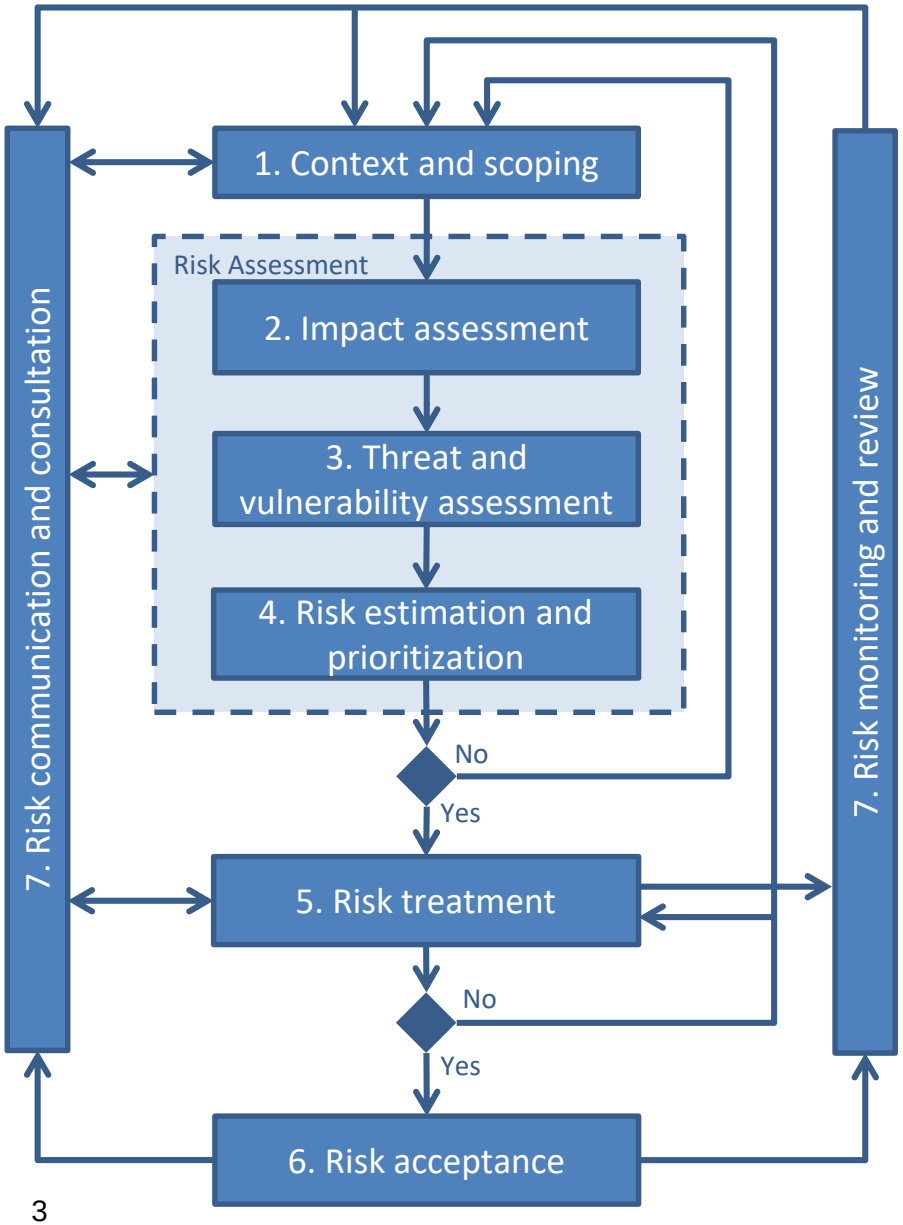
Add new functions to the Power Grid

Development process

new system

time

The SEGRID Risk Management Methodology



- Structured and in-depth methodology designed for Smart Grid risk management
  - To better understand potential threats and vulnerabilities
  - Manage risks
  - Take measures to contain and mitigate risks

Based on ISO/IEC 27005

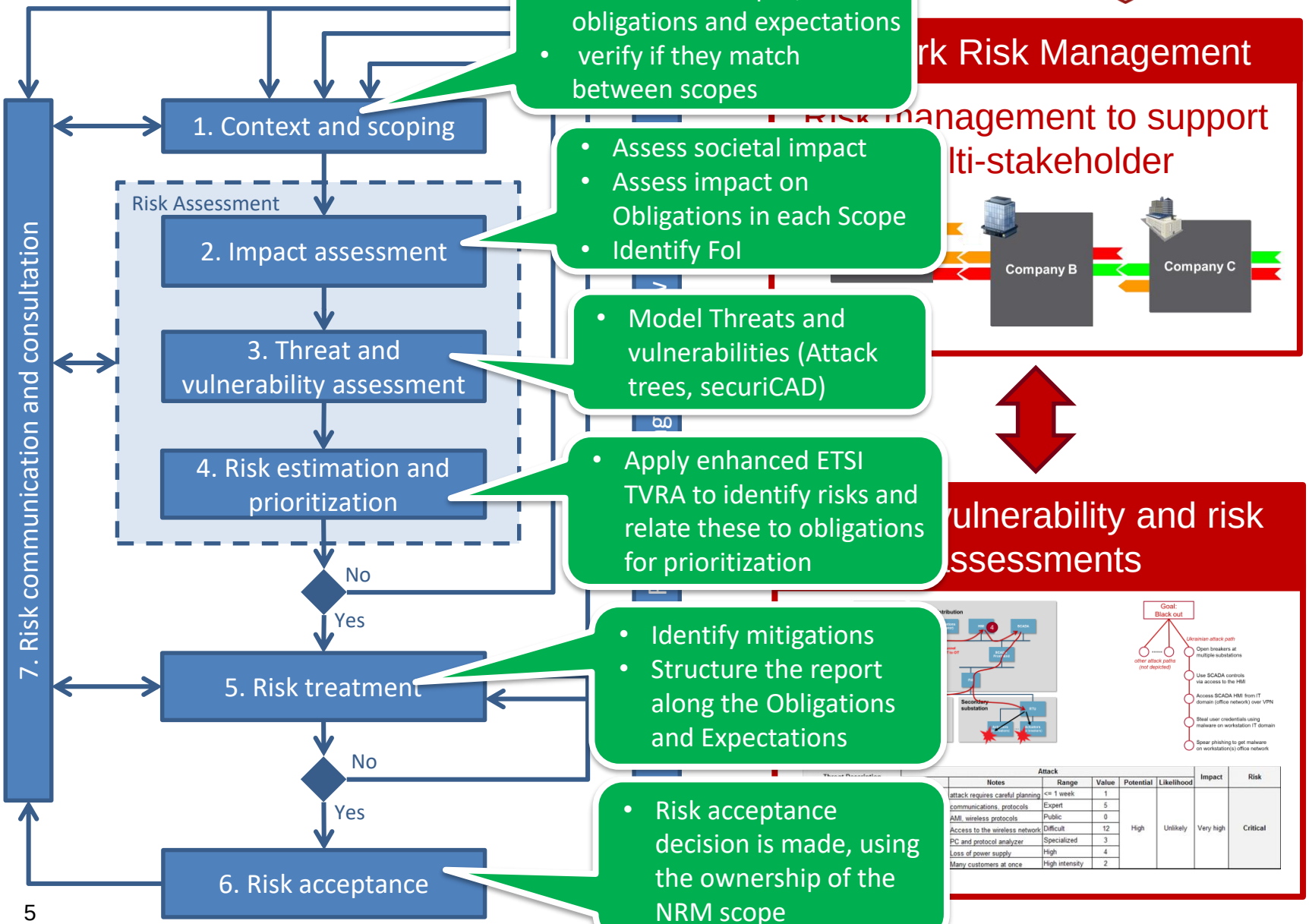
SEGRID Risk Management Methodology

Segrid enhances existing risk-assessment in 3 ways

HMG Information Assurance Standard No. 1 (IS1) as a foundation

- Extends with Network Risk Management Method
  - for insight in dependency, responsibility and propagation of risks in value chains
- Extends the Impact assessment step
  - To include a practical approach to assessing societal impact in the case of a power outage caused by cyber attack
- Applies an enhancement to ETSI Threat, vulnerability and risk assessment
  - to include assessment of the attacker's capability and motivation in the risk-estimation step.

The SEGRID Risk Management Methodology



Applying the SRMM : Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

SEGRID RA scope (DSO)

Society

TSO

Energy supplier

Customer

Software vendor

Telecom operator

DSO

SCADA operations

Work Stations

SCADA

SCADA frontend

Historian

Engineering

Element manager

Update manager

Work station

File transfer server

Internal telecom network

DSO Office

Work station

Office apps

Primary substation

RTU Primary Substation

Actuator

IED

Sensors

Work station

Secondary substation

RTU Secondary Substation

Actuator

IED

Sensors

Work station

DSO AMI

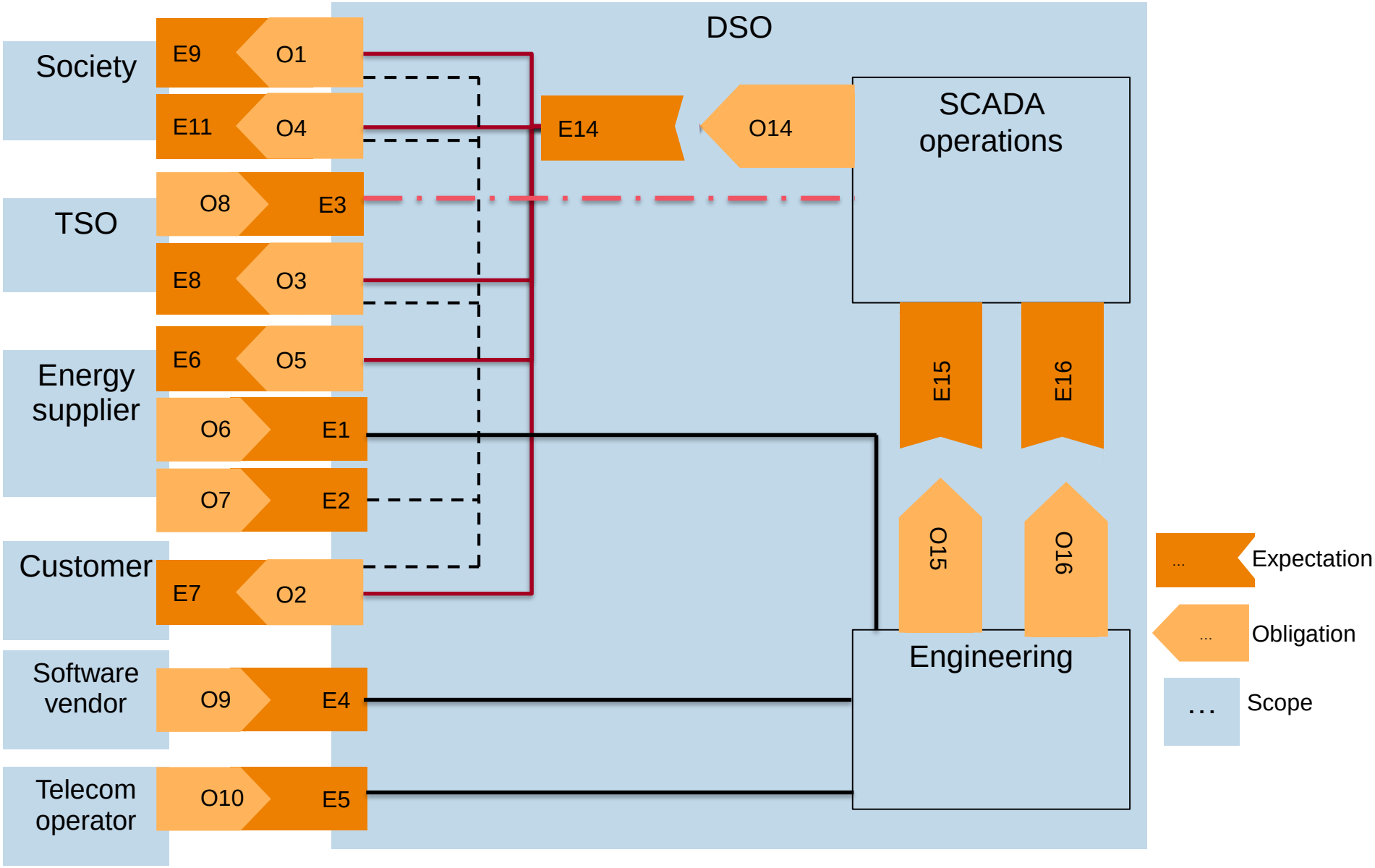
AMI Industrial

Meter data Concentr.

Applying the SRMM : Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

SEGRID RA scope (DSO)



Applying the SRMM : Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

	Obligation		Obligation to scope					
Scope	ID	Name	Energy supplier/ DER	Private Customer	TSO	SW Vendor	Telco	Society
DSO	O1	Avoid failures in the grid						x
	O2	Avoid failures in the grid		x				
	O3	Avoid failures in the grid			x			
	O4	Taking the most advantage of distributed generation						x
	O5	Provide correct setpoints to DER RTU	x					

Applying the SRMM : Use Case 2, Scenario 2

Step 1: Context and Scope of the Risk Assessment

	Expectation							
Scope	ID	Name	Energy supplier/ DER	Private Customer	TSO	SW Vendor	Telco	Society
DSO	E1	Make sensor data available at the DER RTU	x					
	E2	Generation according to setpoints	x					
	E3	Deliver reliable forecast data			x			
	E4	Deliver reliable SW updates				x		
	E5	Deliver reliable communication services					x	

Applying the SRMM : Use Case 2, Scenario 2

Step 2: Impact Assessment

Obligation impact – assessment of maximum impact (worst case) if the obligation is not fulfilled

				Impact if obligation not fulfilled (grey=not applicable)			
ID	Obligation name	Description maximum impact	Maximum Impact	Financial	Reputation	Operations	L&R com-pliance
O1	Avoid failures in the grid	Financial loss, Reputational damage, large impact on operations, high L&R fines	Very high	High	High	Very high	Very high
O2	Avoid failures in the grid	Customers receive no financial compensation, Reputational damage but DSO is monopolist	High	Very low	High		
O3	Avoid failures in the grid	No financial compensation for TSO, TSO will not go public	Low	Low	Low		
O4	Advantage of distributed generation	Mimimal reputational damage, there are some L&R consequences	Medium		Low		Medium
O5	Provide correct setpoints to DER RTU	No financial compensation to DER, considerable reputational damage and operational impact	Medium	Low	Medium	Medium	

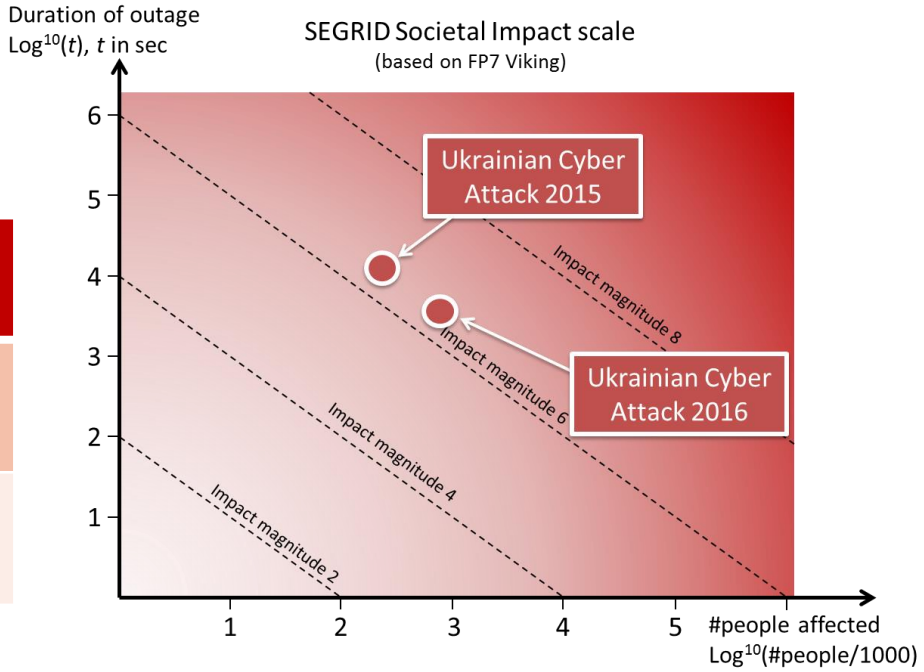
Applying the SRMM : Use Case 2, Scenario 2

Step 2: Impact Assessment

- Societal impact– assessment of maximum impact (worst case) if an attack causes an power outage

	#people affected	Duration
Ukraine Cyber Attack 2015	225.000	1 – 6 hours
Ukraine Cyber Attack 2016	760.000*	1 ¼* hours

* Estimated



SEGRID adopted the approach from FP7 project Viking to plot power outages on Social Impact Magnitude scale and map these to impact scales.

Applying the SRMM : Use Case 2, Scenario 2

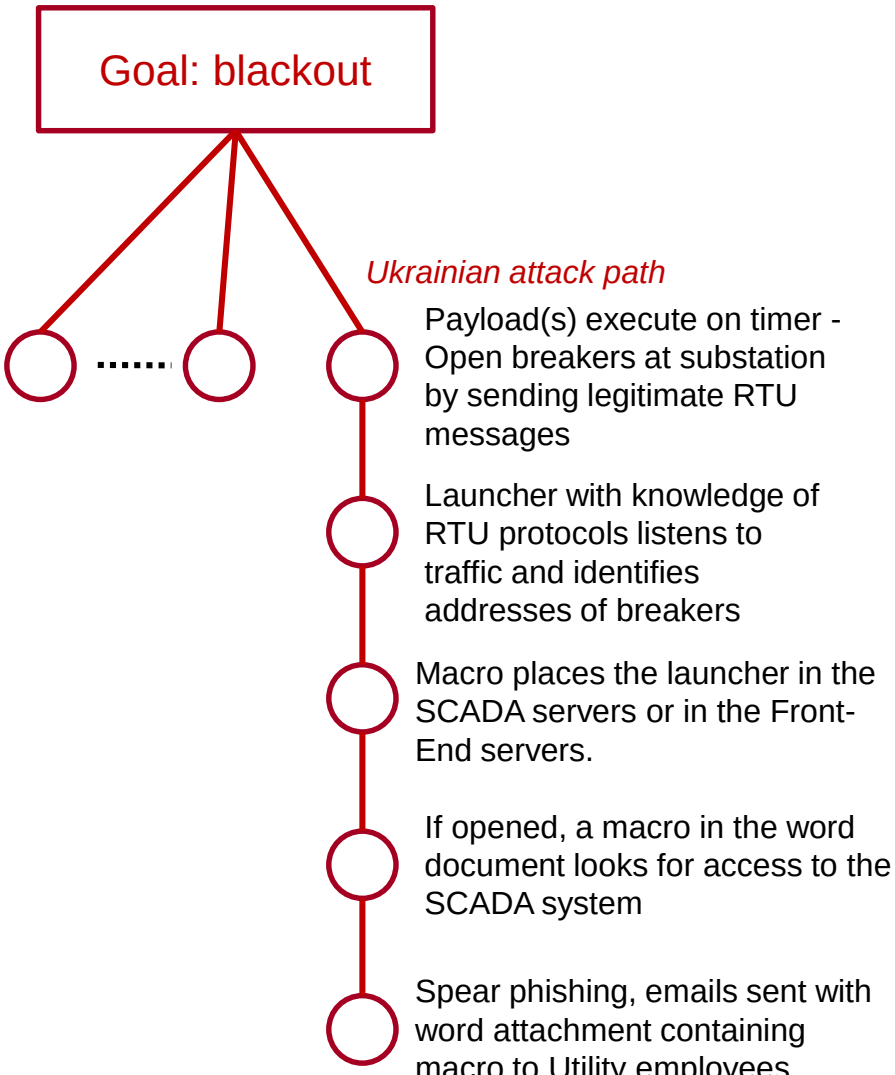
Step 2: Impact Assessment

- The outage's impact can be related to two obligations:
  - O1 - DSO obligation to society – Maximum impact is very high.
  - O2 - DSO obligation to customer – Maximum impact is High.
  - *Due to the relatively short outage, obligations O3, O4 and O5 are not impacted*

Output: identification of the DSO's critical assets in the Focus of Interest

Applying the SRMM : Use Case 2, Scenario 2

Step 3: Threat and Vulnerability Assessment



Description of Threat & Vulnerability Scenario

- Threat: Unauthorized, automated operation of high-voltage breakers
- Assets: SCADA servers, remote terminal units, breakers
- Existing controls: access control, FWs
- Threat source: Unidentified group/Nation State
- Threat actor: Team of highly skilled threat actors
- Threat vector: Spear Phishing attacks to get macro installed at the utility, when Word is opened, the macro starts to look for access to the SCADA system
- Vulnerabilities exploited: Insufficient awareness training, insufficient FWs, or no DMZ
- Threat scenario description: Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in parts of a major city of the attacked country.
- Unwanted incident/event: 760.000 customers lose power for 1 hour and 15 minutes, energy supplier, DSO's and TSOs' operations are impacted, and TSOs' reputation damaged

Applying the SRMM : Use Case 2, Scenario 2

Step 4: Risk Estimation (Risk = likelihood X impact)

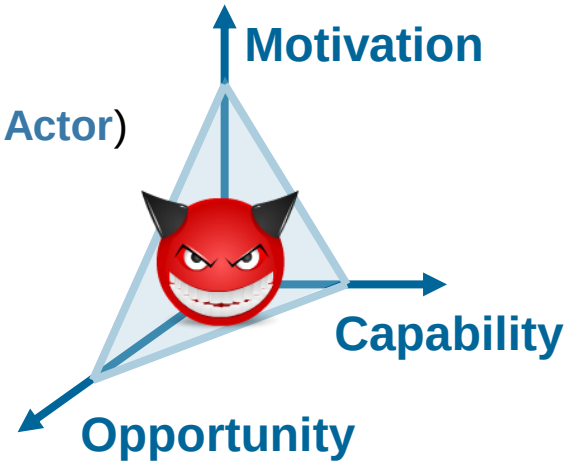
Based on ETSI TS 102 165 & ISO/IEC 18045 – enhanced for SEGRID

- **Attack Likelihood** estimation –
  - Vulnerability rating (**Opportunity and Required Capability**)

    combined with the

  - Threat level (**Motivation & Capability of the Threat Actor**)

- **Impact** estimation –
  - Combines Obligation Impacts



Likelihood Estimation

Attack scenario

Attack Potential	
Time	4
Expertise	6
Knowledge	3
Opportunity	4
Equipment	3
∑	**20**

Vulnerability rating

Likelihood of attack

Threat source/ Threat actor

Property	Capability	Motivation	Threat Level
C	4	3	Moderate
I	4	5	Critical
A	4	4	Severe

Threat Level

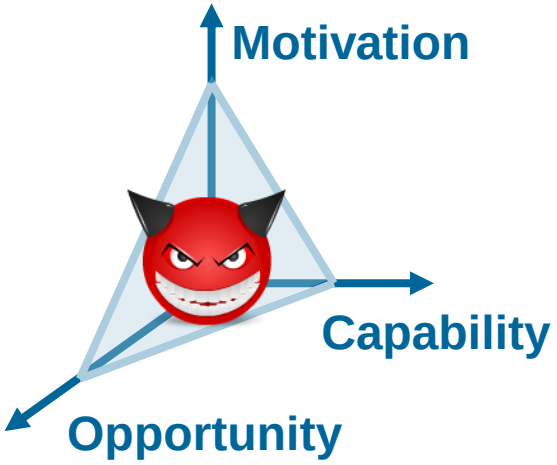
Likehood of attack		Threat Level				
		Negligible	**Low**	**Moderate**	**Severe**	**Critical**
Vulnerability rating	**Basic**	Possible	Likely	Very Likely	Very Likely	Very Likely
	Enhanced Basic	Unlikely	Possible	Likely	Very Likely	Very Likely
	Moderate	Very Unlikely	Unlikely	Possible	Likely	Very Likely
	High	Very Unlikely	Very Unlikely	Unlikely	Possible	Likely
	Beyond high	Very Unlikely	Very Unlikely	Very Unlikely	Unlikely	Possible

Applying the SRMM : Use Case 2, Scenario 2

Step 4: Risk Estimation

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

- **Likelihood** estimation
  - Vulnerability rating (**Opportunity and Required Capability**) is combined with the
  - Threat level (**Motivation & Capability of the Threat Actor**)
- **Impact** estimation
  - Combines Obligation Impacts



Threat Scenario Description	Unwanted Incident or Event	Attack						Impact	Risk
		Factor	Notes	Range	Value	Vulnerability rating	Likelihood		
Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in parts of a major city of the attacked country.	Power outage. 760 000 people lose electrical power for 1 hour and 15 minutes, no physica damage o recovery is quick. Demonstration of capability by threat source.	Time	Planning, several stages of attack	> 6 months	19	f_1			f_3
		Expertise	SCADA experts	Multiple experts	8				
		Knowledge	Knowledge of SCADA protocols, RT	Restricted	3				
		Opportunity	Phishing, insider, for malware delive	Moderate	4	Beyond High	Possible	Very high	Critical
		Equipment	Standard, PC	Standard	0				
		Threat level	Reference threat actor analysis	Critical	4		f_2		
		Impact	760 000 customers lost power, no physical damage	Very high	5				

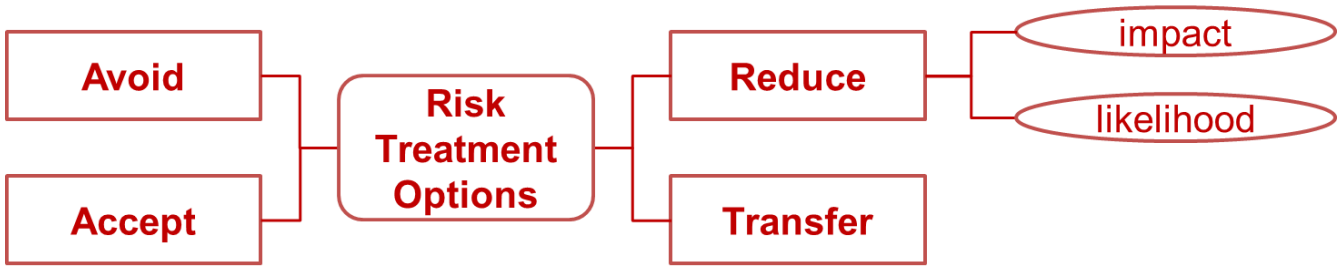
Opportunity

Required Capability

Motivation and Capability of the Threat Actor

Applying the SRMM : Use Case 2, Scenario 2

Step 5: Risk treatment



- For this risk, we choose to Reduce the risk; it exceeds the DSO's risk appetite. We will not accept the risk as-is and there are no possibilities to transfer or avoid this risk.

- Security control selection using IEC 62443-3-3 ⇒ Risk Treatment Plan

ID	Threat	Likelihood	Impact	Risk	Risk Treatment - Selected Security Controls
UKR 2016	Attackers deliver malware launcher to the SCADA zone of the Utility. The launcher has been programmed with knowledge of the RTU protocols used by the utility. The launcher issues commands according to protocol standards to open high voltage breakers which creates blackouts in part of a major city of the attacked country	Possible	Very high	**Critical**	**FR 3: Data integrity** - *Ensure the integrity of the IACS to prevent unauthorized manipulation.* **FR 7: Resource availability** - *Ensure the availability of the control system against the degradation or denial of essential services.* **…**
…	…	…	…	…	…

See SPADE

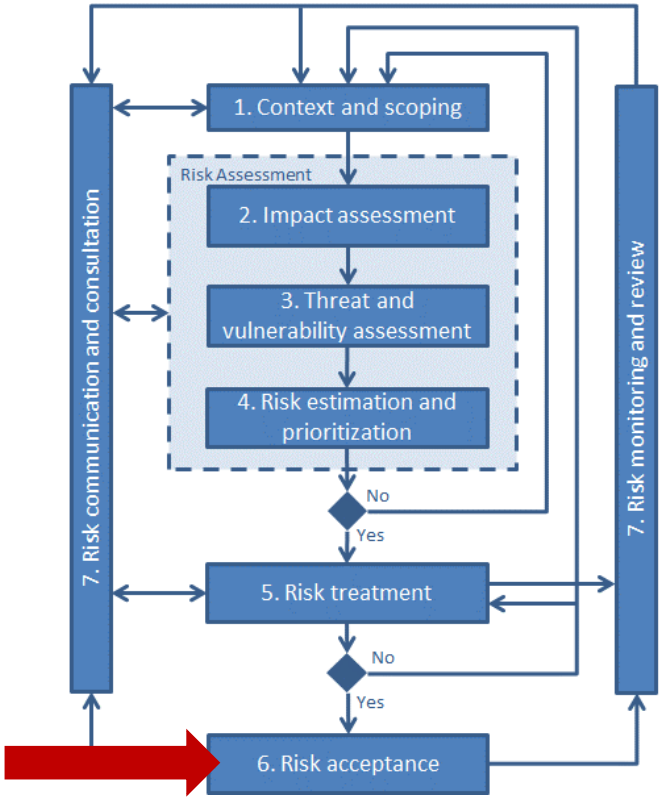
See Cost assessment

Applying the SRMM : Use Case 2, Scenario 2

Step 6: Risk acceptance

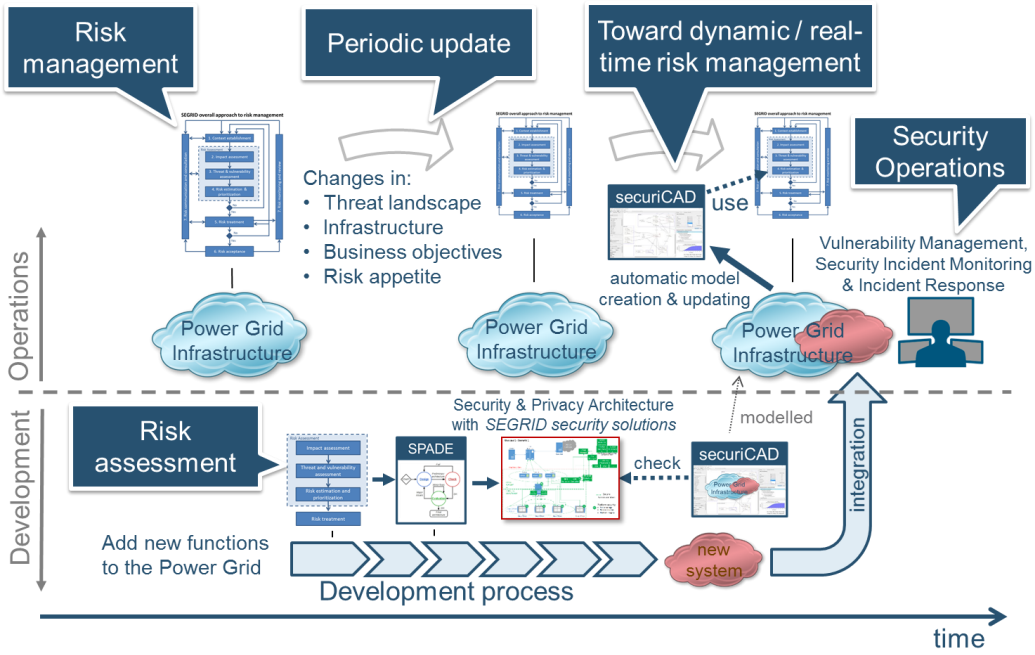
Accept residual risks

- After Risk mitigation plan has been implemented
- By responsible of DSO (DSO director)



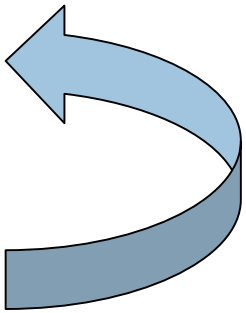
Applying the SRMM : Use Case 2, Scenario 2

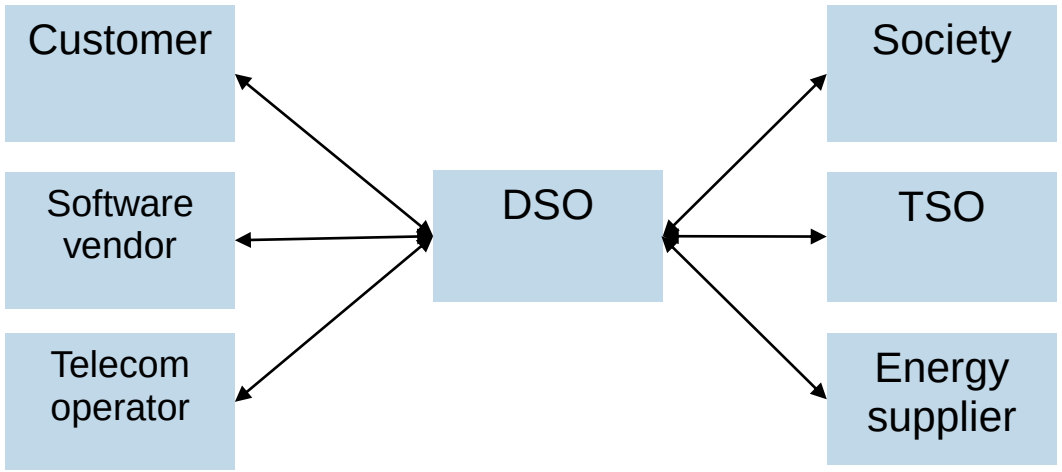
Step 7: Risk communication and consultation



Communicate residual risks

(internally at DSO)





Communicate risks that expectations are not fulfilled

(between stakeholders)

The SEGRID Risk Management Methodology

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

1. Context and scoping

Risk Assessment

2. Impact assessment

- Assess societal impact
- Assess impact on Obligations in each Scope
- Identify FoI

3. Threat and vulnerability assessment

- Model Threats and vulnerabilities (Attack trees, SecuriCAD)

4. Risk estimation and prioritization

- Apply enhanced ETSI TVRA to identify risks and relate these to obligations for prioritization

No

Yes

5. Risk treatment

- Identify mitigations
- Structure the report along the Obligations and Expectations

No

Yes

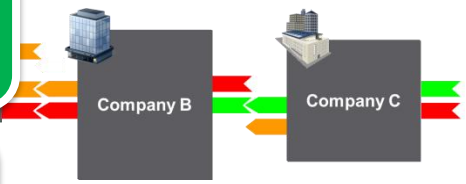
6. Risk acceptance

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

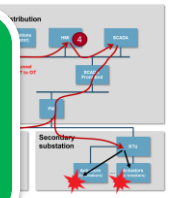
7. Risk communication and consultation

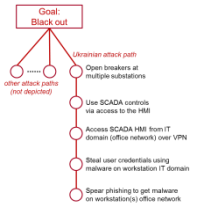
rk Risk Management

anagement to support
lti-stakeholder



ulnerability and risk
ssessments





Attack					Impact	Risk
Notes	Range	Value	Potential	Likelihood		
attack requires careful planning	<= 1 week	1				
communications, protocols	Expert	5				
AMI, wireless protocols	Public	0				
Access to the wireless network	Difficult	12	High	Unlikely	Very high	Critical
PC and protocol analyzer	Specialized	3				
Loss of power supply	High	4				
Many customers at once	High intensity	2				

Concluding remarks

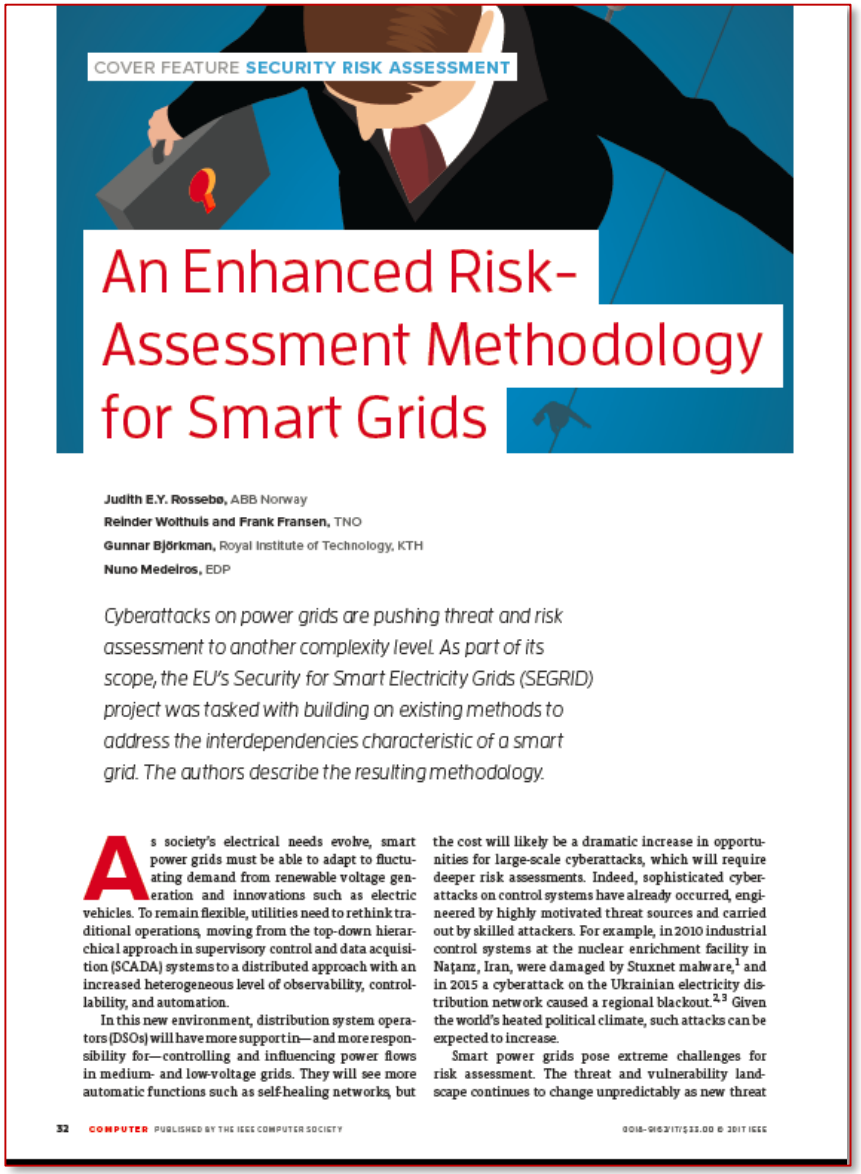
- The SRMM builds on state of the art RA methodologies while providing guidance and enhancements for use in smart grids.

- SEGRID enhances risk assessment in three ways:
  - Including societal impact
  - Including NRM for improved insight in dependencies between stakeholders
  - Including the threat actor motivation and capability in the risk estimation step

- The SEGRID enhancement to the ETSI TVRA has been accepted in the next version of the standard.
  - This ensures that the Threat, Vulnerability and Risk Assessment work will be used

Concluding remarks

You can read more about the SRMM in the April 2017 Issue of IEEE Computer



COVER FEATURE **SECURITY RISK ASSESSMENT**

An Enhanced Risk-Assessment Methodology for Smart Grids

Judith E.Y. Rossebø, ABB Norway
Reinder Wolthuis and Frank Fransen, TNO
Gunnar Björkman, Royal Institute of Technology, KTH
Nuno Medeiros, EDP

Cyberattacks on power grids are pushing threat and risk assessment to another complexity level. As part of its scope, the EU's Security for Smart Electricity Grids (SEGRID) project was tasked with building on existing methods to address the interdependencies characteristic of a smart grid. The authors describe the resulting methodology.

As society's electrical needs evolve, smart power grids must be able to adapt to fluctuating demand from renewable voltage generation and innovations such as electric vehicles. To remain flexible, utilities need to rethink traditional operations, moving from the top-down hierarchical approach in supervisory control and data acquisition (SCADA) systems to a distributed approach with an increased heterogeneous level of observability, controllability, and automation.

In this new environment, distribution system operators (DSOs) will have more support in—and more responsibility for—controlling and influencing power flows in medium- and low-voltage grids. They will see more automatic functions such as self-healing networks, but the cost will likely be a dramatic increase in opportunities for large-scale cyberattacks, which will require deeper risk assessments. Indeed, sophisticated cyberattacks on control systems have already occurred, engineered by highly motivated threat sources and carried out by skilled attackers. For example, in 2010 industrial control systems at the nuclear enrichment facility in Natanz, Iran, were damaged by Stuxnet malware,[1] and in 2015 a cyberattack on the Ukrainian electricity distribution network caused a regional blackout.[2,3] Given the world's heated political climate, such attacks can be expected to increase.

Smart power grids pose extreme challenges for risk assessment. The threat and vulnerability landscape continues to change unpredictably as new threat

0018-9162/17/$33.00 © 2017 IEEE

Thank you

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

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

Reinder Wolthuis
+31 6 5191 33 79
reinder.wolthuis@tno.nl

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