Security for smart Electricity GRIDs

Cost Assessment

Amsterdam, 2 October 2017

Eldine Verweij
TNO The Netherlands

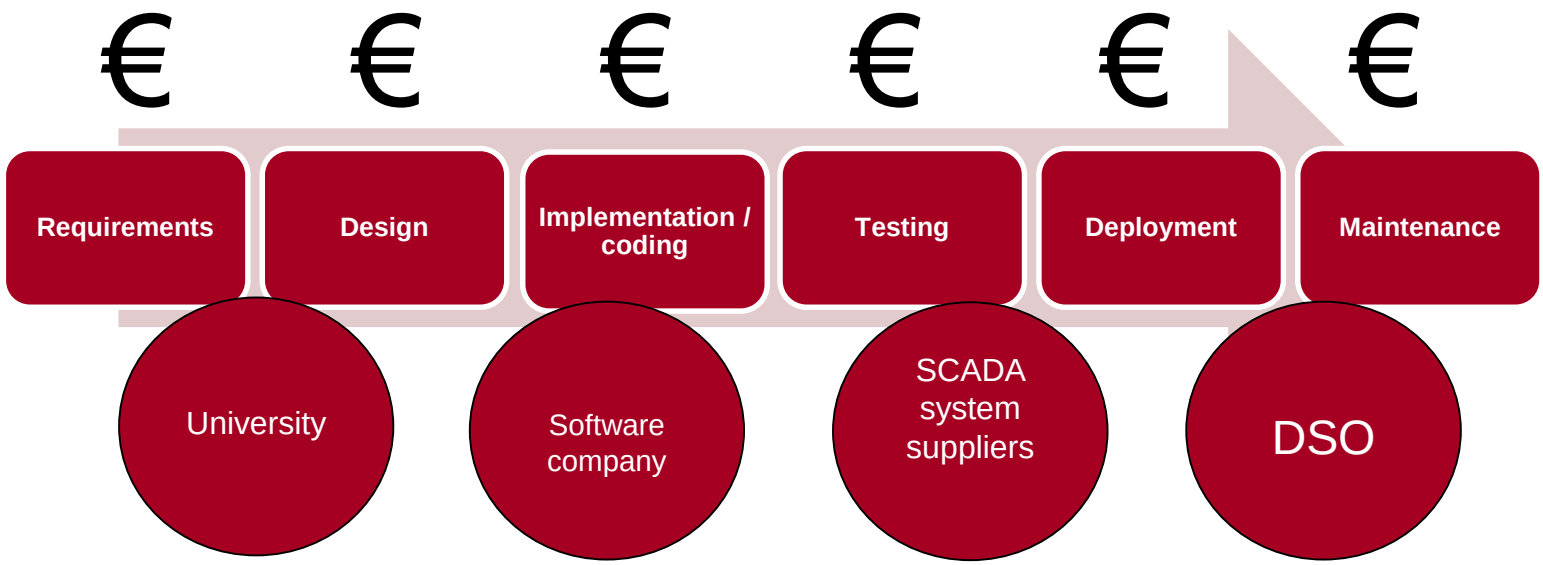
This project has received funding from the European Union's Seventh Framework Programme for research, technological development and demonstration under grant agreement no. 607109

This presentation

- Introduction
- Why cost assessment?
- Cost assessment methodology
- Lessons identified

- Not in this presentation:
  - Numbers
  - Risk reduction

Why cost assessment?



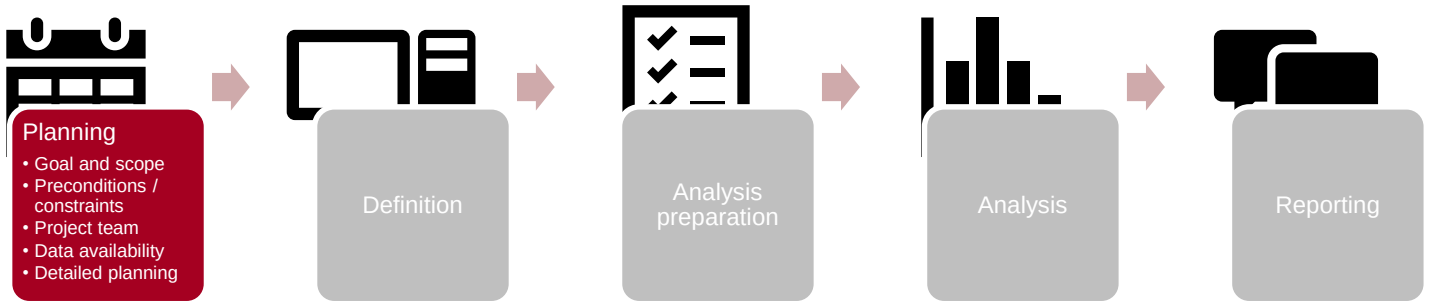
- Support investment decision
- Stakeholder scope: DSO
- Why should this stakeholder invest in a security solution?
  - Cost versus risk reduction trade-off
  - This presentation: cost assessment

Cost assessment methodology

- Primarily based on TNO methodology and EU project VALUESEC
- Consisting of 5 steps

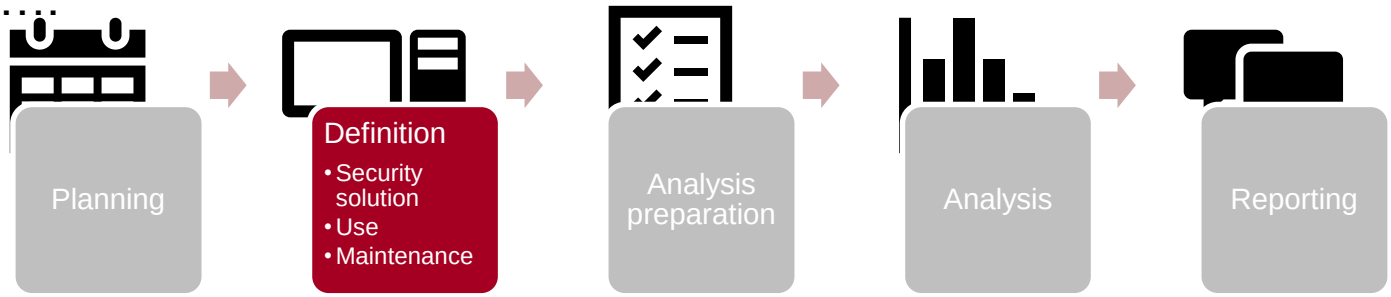
- Security solutions
  - Resilient SCADA systems
  - SecuriCAD based active vulnerability assessment tool
  - Robust scalable (D)TLS based communication
  - Key Management for Group Software Distribution

Cost Assessment Step 1: Planning



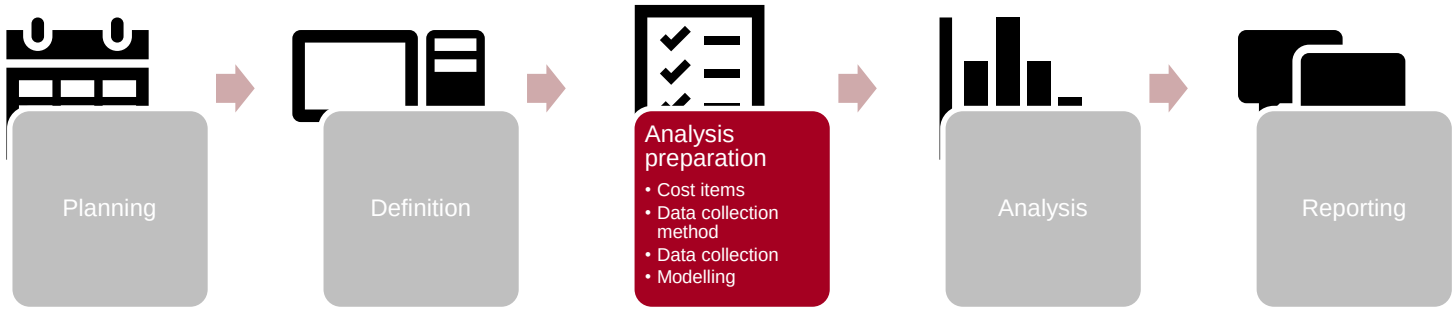
- Goal and scope (p.m.)
- Preconditions and constraints
  - Available budget, lead time, capacity
- Project team
  - Knowledge: financial, technical, project management
- Data availability
  - Experts, literature, databases, accounting systems.
- Detailed planning

Cost Assessment Step 2: Definition



- Security solution definition
  - Included/excluded
  - What is needed for implementation
  - Technical /economical life
  - Organisations involved in use and maintenance
- Use
- Maintenance

Cost Assessment Step 3: Analysis preparation



- Identify relevant cost items
- Data collection methods
- Data collection
- Modelling

Cost Assessment Step 3: Analysis preparation

Identify relevant cost items: Capital Expenditures

For example:

- Network hardware and software (switches, firewalls, DNS, routers)
- Server hardware and software (HP related: servers, storage, racks)
- Workstation hardware and software (PCs, laptops, Office, Messaging)
- Installation and integration of hardware and software, testing (manhours)
- Purchasing research (project costs)
- Initial technology training
- Warranties and licenses
- License tracking – compliance (do I have a correct license for everything, manhours)
- Migration expenses (manhours, user data migration, testing)

Cost Assessment Step 3: Analysis preparation

Identify relevant cost items: Operational Expenditures

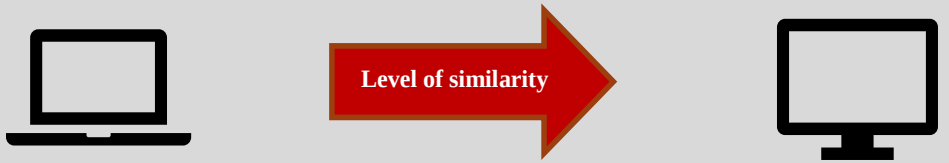
For example:

- Licenses for software and hardware
- (External) Support for soft/hardware (manhours/included in license)
- Internal IT Management and maintenance (FTEs)
- Implement minor changes: upgrades, patches, licenses
- Incident & problem management
- Backup and recovery process
- Infrastructure (floor space)
- Electricity (for related equipment, cooling, backup power)
- Technology training (users and IT Personnel)
- Audit (internal and external)
- Insurance
- Management of IT department(s) / overhead

Cost Assessment Step 3: Analysis preparation

Data collection methods

Analogy:



Parametric:

Analytical:

Costs for initial technology training
=
number of people * average hourly wage * hours needed for training

Expert opinion:

Cost Assessment Step 3: Analysis preparation

Data collection

Data	Industry / developing entity	End or future user*
Security solution	✓	
Use		✓
Maintenance organization		✓
Maintenance	✓	
Organisational setting		✓

*For SEGRID the DSO is the end user

Cost assessment step 3: Analysis preparation

Modelling

Instruction:
This is a generic cost assessment template designed for describing a security solution and its associated life cycle costs.
1. Please fill in the grey coloured fields below. PLEASE BEAR IN MIND THAT YOU SHOULD FILL IN THE ITEMS BELOW FROM A DSO PERSPECTIVE.
2. Definitions of the various items 1 through 6 can be found in tabpage "Definitions".
3. If cost items are not applicable to the solution fill in N/A.
4. If cost items are missing, please insert a new row.
5. If necessary, remarks can be added in column I.
6. For each cost item the lower and upper boundary is requested in column F and G. In case there is no uncertainty please fill in the same

	Resilient SCADA systems	Description of the security solution		
		Specification	Assumptions	Remarks
1	Stakeholder focus			
2	Security solution setting			
	Number of clients served and/or geographical area and/or size etc.			
3	Time horizon			
	Total life cylce of product/service (time till replacement)			
4	Solution definition			
	System definition: what are the elements that make up the security solution: Hardware (e.g. network, server, workstation)			
	Software (e.g. related to network, server, workstation)			
	Solution boundaries: what is specifically not part of the security solution			

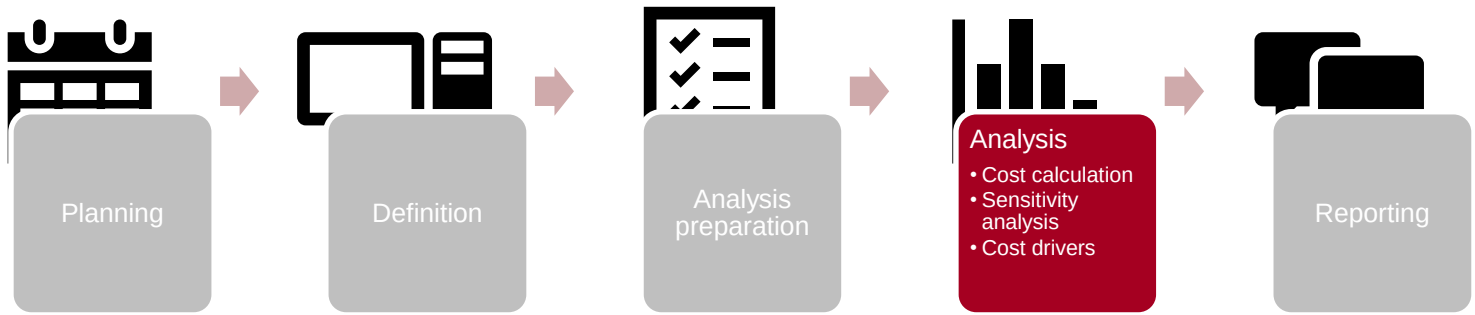
Cost assessment step 3: Analysis preparation

Modelling

Solution procurement and installation costs (€)	Specification	Assumptions	Lower boundary of **total** costs	Upper boundary of **total** costs	Cost source (pick from dropdown list)	Remarks
Elements that can be bought off the shelf						
> Hardware (e.g. number of servers, workstations, networks)						
> Software (e.g. related to number of servers, workstations, networks)						
Elements that require development						
> Hardware (e.g. number of servers, workstations, networks)						
> Software (e.g. related to number of servers, workstations, networks)						
Installation and integration of hardware and software, testing (manhours)						
Migration expenses (manhours, user data migration, testing)						
Decommissioning costs						
Initial technology training (manhours)						
Other project costs (e.g. investigating susceptibility to vulnerabilities, availability of upgrades, patches and future licensing policies, possible costs other stakeholders need to make in order to implement the solution etc.)						
TOTAL			€ -	€ -		

Solution use and maintenance costs (€)	Specification	Assumptions	Lower boundary of **total** costs per year	Upper boundary of **total** costs per year	Cost source (pick from dropdown list)	Remarks
Licenses for software and hardware						
(External) Support for software and hardware (manhours or included in license)						
Internal IT Management and maintenance (FTEs)						
Implement minor changes: upgrades, patches, licenses						
Incident & problem management						
Backup and recovery process						
Data storage						
(Extra) bandwidth						
Infrastructure (floor space)						
Electricity (for related equipment, cooling, backup power)						
Ongoing technology training						
Replacement of hardware (depreciation per year)						
Management of IT department(s) / overhead						
Other recurring costs						
TOTAL			€ -	€ -		

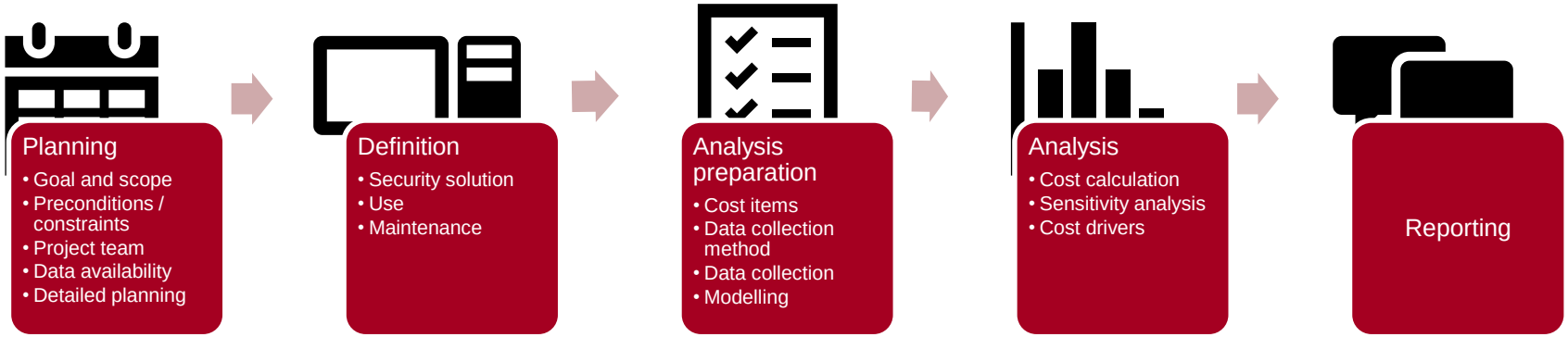
Cost Assessment Step 4: Analysis



- Cost calculation
- Sensitivity analysis
- Cost drivers

Cost Assessment Step 5: Reporting

- Report / Powerpoint presentations
- Graphics
- Include previous steps to clarify validity of outcomes to decision maker



Lessons identified

Planning:

- Involving the right people

Definition:

- Security solution definition & assumptions what is already in place
- Definition of costs items

Analysis preparation

- Market expectations are drivers for cost estimates

Analysis

- New solutions: lots of best guesses and cost uncertainty
- Context specific outcomes

MAKE ASSUMPTIONS EXPLICIT!

Questions

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