ENERGY SHIELD

Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of critical Energy Infrastructures

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

WP8 EXPLOITATION & SCALE UP

D8.4 BUSINESS CASES

Document info	
Contractual delivery	2022-04-30
Actual delivery	2022-04-30
Responsible Beneficiary	PSI Software AG
Contributing beneficiaries	All partners
Version	1.0
Dissemination Level	Public

This project has received funding from the European Union's H2020 research and innovation programme under the Grant Agreement No. 832907

DOCUMENT INFO

Document ID:	D8.4
Version date:	2022-04-30
Total number of pages:	76
Abstract:	This Deliverable D8.4 summarizes the results from Task 8.2 “Business Cases” and describes the industrial business cases development for the EnergyShield toolkit, including return on investment (ROI) and cost-benefit-analysis (CBA). The task 8.2 will leverage the results of the pilot to evaluate the potential benefits (and costs) of rolling-out the EnergyShield solution within the entire organization of an EPES operator (and its supply chain). Industrial business cases will not contain sensitive information about critical infrastructure operations, so they can be made public and serve as a dissemination collateral in order to convince other EPES operators to adopt the solution.
Keywords	ROI, Costs, Benefits, Business Case, Exploitation

REVIEWERS

Name	Organization	Role
Magda Zafeiropoulou	SC	Overall Reviewer
Maria Atanasova	SC	Overall Reviewer
Per Eliasson	FOR	QA Reviewer
Joakim Nydren	FOR	QA Reviewer

AUTHORS

Name	Organization	Role
Amir Kandell	SIGA	Contributor
Ariadni Michalitsi-Psarrou	NTUA	Contributor
Christos Angelidis	KT	Contributor
Gianluca Serale	IREN	Contributor
Hagai Galili	SIGA	Contributor
Joakim Nydren	FOR	Contributor
Karsten Natusch	PSI	Contributor
Matthias Rohr	PSI	Overall Editor & Contributor
Stefan Wietzke	PSI	Contributor
Yisrael Gross	L7D	Contributor

VERSION HISTORY

0.01	2022-01-11	Initial version
0.02	2022-01-14	Approach draft
0.03	2022-01-25	Business case outline
0.04	2022-02-03	Scenario for “roll out”
0.05	2022-02-14	Survey for large users (DSO/TSO)
0.06	2022-02-14	Survey for GENCOs
0.07	2022-02-24	Survey for tool providers
0.08	2022-03-11	Rollout scenarios
0.09	2022-03-14	Market size estimation
0.10	2022-03-14	Market size estimation
0.11	2022-03-17	Analysis of cost and benefits
0.12	2022-03-11	Renewed Surveys
0.13	2022-03-25	Integration from survey answers
0.14	2022-03-25	Adjustments on scenarios
0.15	2022-03-30	Market size estimation adjustments
0.16	2022-04-04	Scenario for typical customer
0.18	2022-04-12	Quantification of benefits and costs
0.19	2022-04-18	Integration of more survey results
0.20	2022-04-19	Computation of CBA and ROI
0.21	2022-04-20	Combining parts for reviews
0.22	2022-04-22	Discussions
0.23 – 0.34	2022-04-24 – 2022-04-30	Completion of the deliverable and work based on the comments from the reviewers
1.00	2022-04-30	Final version, released to the EC

EXECUTIVE SUMMARY

This report describes costs and benefits of the EnergyShield toolkit with a focus on the customer's point of view and analyses business case scenarios for the toolkit.

The report uses experiences from the toolkit instantiations in the field trials and from literature research to conduct a cost and benefit analysis and a calculation of the return-on-investment (ROI) for the roll out of the EnergyShield toolkit.

The ROI analysis addresses:

- Data breach incidents and incidents that cause electrical power outages
- Distribution system operators of different size (1,5 and 3 million households)
- Financial costs for the initial victim of the attack and for the general public
- The influence of cybersecurity insurances and liability

For the larger company scenario, the ROI is slightly in favor for the EnergyShield toolkit even under purely financial evaluation. The ROI is positive for smaller energy companies if some cyber-attack damages of the public are included.

The business case analysis defines the focus energy market segment and estimates its size of 558 energy sector companies with more than in total 800.000 employees in the EU and in the countries of the project partners.

Additionally, three different business case scenarios and their possible outcomes are studied. Two show good business opportunities for the EnergyShield toolkit.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

ACRONYMS

ACRONYM	DESCRIPTION
AD	Anomaly detection
B2C	Business-to-consumer
BC	Business Case
BMC	Business Model Canvas
CBA	Cost-benefit analysis
DDoS	Distributed Denial of Service
DDoSM	Distributed Denial of Service Mitigation
DSO	Distribution System Operator
EPES	Electrical Power and Energy System
ES	EnergyShield
GDP	Gross domestic product
GDPR	General Data Protection Regulation
GenCo	Power Generation Company
HV	High Voltage
KPI	Key performance indicator
LV	Low Voltage
MV	Medium Voltage
OT	Operational technology
ROI	Return on investment
SBA	Security Behavior Awareness
SIEM	Security Information and Event Management
TSO	Transmission System Operator
USP	Unique Selling Points
VA	Vulnerability analysis

1. INTRODUCTION

1.1. SCOPE AND OBJECTIVES

In the context of WP8 Exploitation & Scale Up, this document targets business cases, return on investment, and cost benefit analysis of the Energy Shield toolkit and concludes results from Task 8.2. It complements the previous business model canvas (deliverable 8.2 [ESD82]) by addressing and quantifying the value of the EnergyShield toolkit to potential customers.

The experiences from the toolkit instantiation within the EnergyShield project and literature research allow us to make estimations on larger rollouts of the EnergyShield toolkit into production systems and to quantify the expected benefits.

This document supports EPES operators in their evaluation of the EnergyShield toolkit. Toolkit providers and regulators can get an understanding how the costs and benefits meet in the ROI analysis in the context of two cyber incidents in two different energy sector companies. This report can provide input for standardization and regulation authorities that want to enable a suitable business environment for additional security products.

In context of business case analysis, three possible future scenarios are described and financially analyzed. Neither sensitive information from the field test users nor business internals of the tool providers are disclosed to make this document available to potential users, partners, or others that are interested in the EnergyShield toolkit.

Results from this document will especially influence the ongoing business case discussions, influence the final exploitation strategy, and will help to provide and discuss offers to new potential users in the post-project period.

1.2. STRUCTURE OF THE REPORT

The report is structured as follows:

- Section 2 describes the strategy how the task of this deliverable is approached and how the main parts Section 3 and Section 3.6.3 are connected.
- Section 3 takes the users perspective with a **Return-on-Invest** (ROI) and **Cost-Benefit-Analysis** (CBA). This especially provides financial and quantitative arguments for potential customers of the EnergyShield toolkit. Additionally, it explores and demonstrates a possible pricing scheme for projects (without revealing too much internal details, such as costs and margin).
- Section 4 analyzes quantitative aspects of the **Business Case** (BC) for the EnergyShield toolkit as instantiation of the example joint business model. It is a quantitative analysis from the perspective of the EnergyShield toolkit provider and of the EnergyShield project partners.

- Section 5 concludes this report with a summary of the most important results, a discussion of major assumptions and limitations and next steps.
- Sections 6 - 9 contain references and Appendixes.

1.3. TASK DEPENDENCIES

Important inputs (ingoing dependencies) for this task are:

- **WP2 – WP4**, which create, extend, and adapt the tools of the toolkit. For the analysis of costs and benefits, it is relevant to identify the costs and benefits especially from the EPES-customizations.
- **WP1**, which defines the requirements and architecture for the toolkit. The tools and the toolkit are the major results for the exploitation. Especially the identification of the commercial requirements resulted in some market assumptions that are used in this deliverable.
- **WP5**, which integrates the tools into a toolkit. The concrete integration concept defines possible synergies regarding costs and benefits in contrast to providing a set of single tools.
- **WP6**, which is about the field trials. Some preliminary insights from the field trials are considered in this report. This is under some limitations because, firstly the field trial results D6.3 (Field trial evaluation report) and D6.4 (penetration testing reports) are due after the creation of this deliverable, secondly, D6.3 is strictly classified by the Grant Agreement and results are not to be used in this report, thirdly, the field trials are still under evaluation, and finally because the field trial are a first test of the toolkit and only to a limited extent comparable to a roll-out scenario. However, this report involved discussions and a questionnaire with both tool providers and users (i.e., the energy companies) that participated in the field trials, so that some general experiences are included in this document.
- **WP8** provided major starting points for this deliverable in the deliverable D8.2 [ESD82], such as the first parts of the business canvas analysis, the USPs of the EnergyShield toolkit, a market overview on cybersecurity toolkits and related tools, defined customer segments, the example business model used in the business cases and the price model.

Outputs of the task are:

- The results of the work on the business cases especially influence the remaining work on the exploitation strategy which is the subject of **WP8** Task 8.1 (Develop the exploitation strategy and plan).
- Some insights of this reports are a subject for communication and discussion with potential customers. These aspects are related to **WP7** Task 7.3 Market dissemination and ecosystem development.

- Other insights on the role of regulation and the market mechanisms discussed in the CBA and ROI analysis can be relevant for discussion with standardization and regulation bodies, which are subject of **WP8's task 8.4** (Manage standardization and regulatory aspects).

2. APPROACH

The approach of this report is to complement the previous results of the EnergyShield project with a quantitative and financial analysis. It provides a cost-benefit analysis, a return on investment, and financial business case aspects. This analysis is based on assumptions, project internal experience collected by a questionnaire, and literature research. The results are expected to be to some extend explorative, but all these sources are combined to quantify the value of the EnergyShield-Toolkit and its cost in a full rollout scenario and the potential market demand to explore business cases.

General limitations for the scope of this report:

- The analysis of costs and benefits is focused to TSOs, DSOs, and GENCOs in the European electrical energy sectors, because these are best presented in the field trials and by the project partners in the EnergyShield project.
- Medium/large DSOs are defined as example customer scenario for the CBA/ROI, because DSO have both critical OT systems that organize the electrical supply of the general public and have IT systems with many records of private customer data. This allows to model and study both attacks that aim for power blackouts, ransomware attacks, and possible GDPR violations.
- CBA, ROI, and BC are all evaluated for the entire EnergyShield toolkit and its joint business model. Single tool price calculations and single quantitative business case details of the toolkit providers are not presented to not reveal business internals.
- The internal costs and the margin of the EnergyShield toolkit general contractor and integrator role and other central EnergyShield roles are not revealed in this public report, because it reduces business success chances, if, for instance, the minimum acceptable price can be estimated by potential customers.

2.1. COST-BENEFIT ANALYSIS AND RETURN ON INVESTMENT

We follow the approach of [PPP19] and [PPP08] to create the ROI based on the CBA, since both depend on cost and value estimations. The Grant Agreement desires the CBA/ROI based on a rollout scenario, which is first to be defined (for each tool).

Following steps are performed by the CBA and the ROI analysis:

- Identification of CBA and ROI structure, and perspectives
- Definition of typical example **customer scenario** as perspective for CBA/ROI
- Identification of **toolkit impacts** that create costs and benefits
- **Quantification of cost and benefits** for the calculation of the financial **CBA**
- Calculation of the financial **ROI** based on financial CBA
- Analysis of outcomes

2.1.1. REDUCED CYBER RISKS AS BENEFITS

The analysis of benefit of the EnergyShield toolkit is special because the primary benefit is to reduce potential risks and consequences from cybersecurity attacks to energy companies. Therefore, we explore in more detail the potential costs and consequences of attacks to grid operators and other energy companies. This also corresponds to an open key point of our BMC (business model canvas) – what is the actual value of a product.

2.1.2. RISKS TO THE PUBLIC

This document also evaluates costs that currently have to be borne by the general public. This allows to study the CBA/ROI and the value of the toolkit in a broader scope – which is relevant since many energy sector companies are state-owned and regulated to meet the needs of the general public.

2.2. BUSINESS CASE ANALYSIS

In contrast to the CBA and ROI, which take the perspective of the customer, the business model will take the perspective of the EnergyShield toolkit provider to the customer. This quantitatively evaluates and completes the business model created with the business model canvas analysis in [ESD82].

The business case analysis follows the following steps:

- Business case assumptions based on previous work
- **Market estimation**
- Evaluation of **business case scenarios**
- Analysis of outcomes

2.2.1. BUSINESS MODEL CANVAS

This deliverable complements the application of the Business Model Canvas [OP10], which is illustrated in Figure 1. Sectors 1 to 5 of Figure 1 have been covered by Deliverable 8.2 [ESD82] – this report especially addresses sectors 1, 2, 5 as highlighted in the deliverable and with a focus on quantitative data. Sector 9 has been internally evaluated to make price calculations possible, but will not quantitatively revealed as discussed on page 14. However, the price example calculation will make the flow of money within the business model transparent. The other sectors have been covered by other EnergyShield reports.

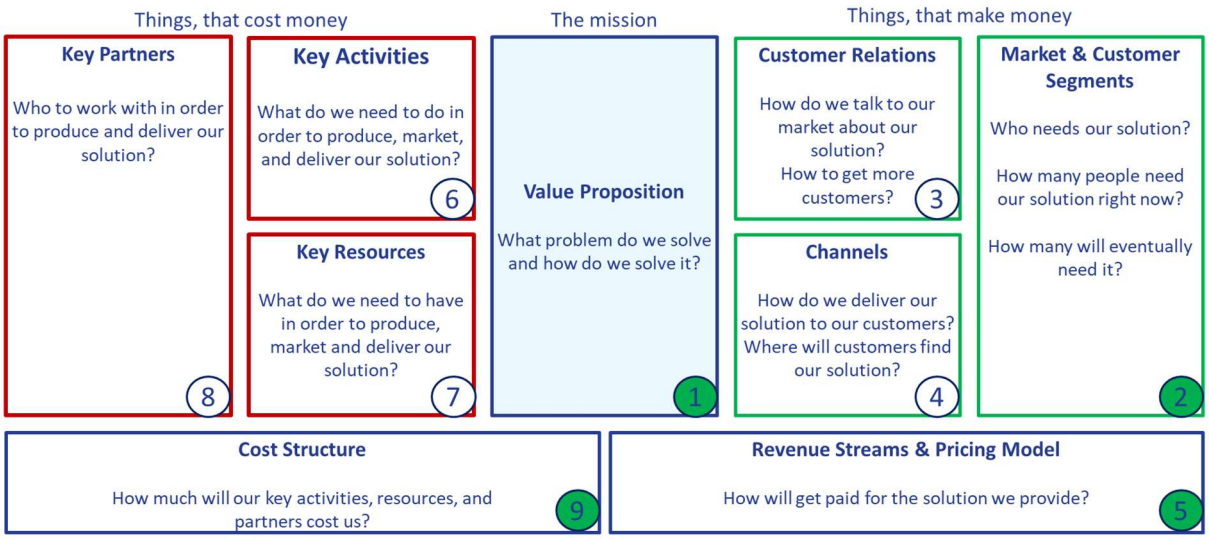

Figure 1: Overview on the areas and fields of the Business Model Canvas addressed (based on [OP10]) – the green numbers indicate the focus of this deliverable.

2.2.2. TARGET MARKET SIZE ESTIMATION

A new estimation of the primary target market size is provided based on socio-economic data. It is based on previous analyses (e.g., customer target segment analysis for each tool and USP analysis of the toolkit) in previous work within the project, which studied in detail which types of customers would have most benefit and be most promising to be targeted.

3. COST-BENEFIT-ANALYSIS & RETURN-ON-INVESTMENT

This section studies costs and benefits of the EnergyShield toolkit both from a customer's and toolkit provider's perspective, with a focus on the customer's perspective. The costs and quantifies are analyzed and quantified to compute the return-on-investment. The financial costs and benefits and the financial ROI are evaluated in a defined project context and for defined assumptions. As requested by the EnergyShield Grant Agreement, the task is not to look at small-scale pilot projects (which are often typical for new technology in the energy sectors) but to look more at a "roll out", because a small-scale scenario is already covered by the field trials. The scale of the reasonable roll-out scenario considered in the CBA is described for the toolkit and the five tools in 3.5.2.

3.1. GENERAL BENEFITS FROM THE TOOLKIT

Since other EnergyShield publications focus on the functional benefits of the tools and of the toolkit in detail, only a short summary of selected benefits and outcomes are provided.

Examples for potential short-term benefits:

- The EnergyShield DDoSM (Distributed Denial of Service Mitigation) protects several important external APIs.
- The EnergyShield AD (Anomaly Detection) protects the most critical OT from Stuxnet-like attacks that could damage equipment or lead to unplanned power outages.
- The EnergyShield SBA (Security Behavior Awareness) addresses the security awareness of the toolkit customer's employees.
- The EnergyShield VA (Vulnerability Analysis and Threat simulation) might reveal unknown structural security issues during the initial model creation and simulation.
- The EnergyShield SIEM (Security Information and Event Management) provides an integral security status across all security-related issues and enables targeted and controlled crisis intervention in real time.
- The tools together provide faster/better detection of multi-vector attacks and higher chances of interrupting attacks.

Examples for potential medium-term and long-term benefits:

- Improved security culture and security awareness addresses the highly relevant "human factor" in cyber security.
- VA helps to iteratively maximize the efficiency from new security invests
- Reduction of the risk for the general public for black outs and for energy data breaches

- The stress level for the IT and security employees of the EPES company is reduced and it is easier to get good employees to work in a state-of-the-art-environment
- It is intended that the EnergyShield toolkit will support more and more tools over the time. Existing toolkit customers can add such new tools to their toolkit instance much more easily and with lower effort compared to customers that do not have a toolkit.

3.2. BENEFITS COMPARED TO INDEPENDENT TOOLS

3.2.1. LESS EFFORT FOR THE CUSTOMER IN PROCUREMENT, SPECIFICATION, INSTALLATION AND OPERATION

A benefit for the customer of the EnergyShield toolkit can arise because the procurement, specification installation, and operation might require less effort on the customer-side compared to the processes for several individual tools. This is especially beneficial if own capacities (e.g., IT-, security teams and related decision makers) are already working at full capacity to deal with the continuously growing security risks and requirements. In addition, the operation and protection of IT systems is not the core competence of physical infrastructure operators. Improving the ability to cope with complexity is therefore essential in order not to lose the company's focus. And the best way to do this is to outsource complexity to third parties.

We experienced that the customer's own expenses for the introduction, operation, and maintenance of IT systems are regularly underestimated. [HLA03] provided a study on two-dozen contracted software projects. It showed that substantial costs are on the side of the customer: almost twice as much cost (190%) of the contract cost resulted on side of the customer as these "hidden costs". The costs especially resulted from user effort and project management effort participating in the analysis, design, testing, and implementation phases [HLA03]. We expect lower hidden costs in our scenario because the toolkit is provided out of software products and not a software development project, but still we assume that there is a significant customer effort that is usually not measured.

We estimate that the platform provides potential synergies in the specification and installation, operation, and maintenance of 5% - 30% (average 16%) of the initial tool project cost, if three or more tools are installed.

The following subsections discuss these benefits in more detail.

3.2.1.1. SYNERGIES IN THE PROCUREMENT PROCESS

Software procurement consists of many points (e.g., see [AAM17]), such as involvement of all internal stakeholders, definition of requirements and selection

criteria, finding potential products (reverse marketing), evaluation of the product, evaluation of the vendor, negotiation of financial and non-financial contractual. Many energy companies might be public companies and must fulfil special procurement requirements. Additionally, especially cybersecurity tools in the energy sector could be subject to the guidelines published by ENISA publication on “Indispensable baseline security requirements for the procurement of secure ICT products and services” [ENI16]. Even more effort results from implementing the requirements to evaluate the complete supply-chain (i.e., not only the evaluating the vendor but also the vendor’s vendors, and so on), as recommended for instance, by [ENI16]. Additionally, purchase regulation might apply from the EU Utilities Directive, or the Public Sector Directive as pointed out in [SOE11].

Special issues from cyber security tool procurement might difficulties to evaluate the effectiveness of a tool (special knowledge required) and to oversee all potential side effects (e.g., maintenance efforts for renewing certificates).

If individual parts are procured, it is not only the integration risks that usually lies entirely with the procuring company. This includes not only the technical implementation but also different contract constructions, business, and price models, as well as release cycles and technologies. The corresponding effort grows exponentially.

We conclude – making one large procurement process for a cybersecurity toolkit can be significant less effort than making several procurement processes for independent tools that must work together.

3.2.1.2. SPECIFICATION AND INSTALLATION PHASE

Even if the products would be plug-and-play, still the IT- and security departments would need to be involved in the definition how the tools operate in your environment, and some IT-requirements, such as network connections, firewall settings, VPN configuration, setting up a remote maintenance access, would all have to be discussed. Especially in larger organizations, it can be quite time consuming just to identify all people, that must be involved in the installation phase at some point and to agree to simple basics, such as get clearance to use a certain database library or operating system on a server.

3.2.1.3. OPERATION AND MAINTENANCE

Maintenance costs from the perspective of the customer (e.g., a utility company) can be a significant portion of the total costs of a software or software/hardware product. In this discussion we consider the maintenance costs as the sum of:

- External maintenance costs that the customer pays to the vendor/operators of the EnergyShield toolkit.
- Internal maintenance costs of the customer primarily resulting from the effort of own employees. This includes aspects such as contract management, supplier

management, software management, identification of the corresponding vendor in case of a failure, entering and tracking of failures in ticket management systems, contacting the vendor regarding a failure, software auditing, creation and testing of backup for the software, management and installation of available updates and upgrades for the software.

From a software development perspective, maintenance costs have for instance, been reported in the range of 50% to 90% of the total software lifecycle costs [AAP10]. Of course, there is a difference between the vendors' cost perspective and the customer's cost perspective, but usually there are some correlations. However, several points let us assume that security products in the energy sectors provide good chances for vendors to reclaim his maintenance costs from the customer:

- Especially security products must be up to date because of the continuous competition between security product vendors and attackers. Some security products, such as virus scanners make no sense without a maintenance contract that provides up-to-date virus signatures.
- Many energy sector companies follow procurement processes (e.g., public tenders) that put a lot of pressure and focus on the negotiation of the initial price. Additional pressure on the initial project price might result from the difficulties for evaluating the quality and capabilities of different security products for a customer. Some markets outbalance low initial prices with higher prices for maintenance or extensions. Since some security products such as a SIEM or OT-Anomaly Detection tool cannot be easily replaced, the negotiation position of a vendor is better after the initial project for claiming a fair price than during a tender for the initial project. [CKS15] observed from several studies that major global information technology had "large relative increases in maintenance and other product-related services [...] as sales of their product lines have declined or as product prices have fallen".

Some security products need a lot of individual configuration or adaptation to the customer's specific environment and lead to high maintenance effort. For instance, the roll out of a SIEM system will require specific probes and integration of essential systems (e.g., system specific log files or health checks). Therefore, a SIEM installation project typically requires a lot of "development" in terms of configuration. This development can be done by external consultants or by internal employees. In any case, the custom configuration files, data models, dashboards, reports and setting all need to be (usually manually) maintained to cope with changes in the system landscape.

There are several points of the EnergyShield toolkit that let us assume that the maintenance effort on behalf of the customer will be lower for the EnergyShield toolkit with several tools than for independent tools from different vendors. More precisely, it is assumed that the EnergyShield toolkit can scale better with a growing number of security tools:

- The EnergyShield toolkit only requires one remote access point for all tools. If tools are from independent vendors, each one might require its own remote access point. Every remote access point requires attention and therefore effort from the IT- and security department of the utility for both the initial setup and the continuous operation. Additionally, each remote access point often leads to third party costs for its own protection (such as license costs for VPN, remote desktop, firewall, end point protection, and DDoSM).
- The EnergyShield toolkit has shared infrastructure. The tools and the EnergyShield portal share technology such as messaging, databases, container management etc. These components need their regular security updates and other services, such as checking the backups and verifying correct operation from time to time. It is likely that many independent tools will have many more components that need their regular updates, validation, backups etc. which results in more effort for the utilities' own IT or maintenance costs if this is outsourced. If all tools use for instance, the same database, only one data backup and recovery strategy needs to be implemented.
- One possible EnergyShield toolkit contract could provide a single point of (initial) contact for troubleshooting and support calls. This reduces on the customer's side the effort to identify who to contact for a failure. Additionally, the EnergyShield toolkit provider will help to take care that the tools operate together – this is a typical problem for independent tools: each vendor might blame the other vendor for an integration problem and the customer has effort to figure out the technical and contractual responsibility for an integration problem. This kind of "**blame game**" was for instance, described by [ACT16] for occasional reboots in Microsoft's data center, which can have many root causes. Especially for a customer of software and IT, it can be very challenging to find the responsible party for certain types of failures that result from the interaction between systems because of both technical and contractual complexity. For instance, a single tool on a shared machine that consumes all free memory or CPU might lead to a crash off all tools – it could be each tool on the server that caused the crash, and each customer support might at first claim that they don't think it their responsibility. Several categories of bugs, such as memory leaks can be very difficult to locate [PRS07]. One strategy to avoid the blame game, is to contract large areas of responsibility to a single service provider.
- The EnergyShield toolkit support will be familiar with both the toolkit technology and the energy sector domain specific. Therefore, the maintenance support of energy sector specific trouble calls will require less effort on side of the utility and less effort on the side of the EnergyShield support provider. For instance, a trouble call "we don't get new measurements into the billing" could be resolved by an EnergyShield support technician by "first: can you look into the SIEM if the AMI-public-endpoint is operational; second: let us check the DDoSM-API protection – there might have been an attack against this public interface". A non-domain-

aware single-product-support engineer will first have to figure out what billing means for a utility, that this has to do with the public-AMI-API and that this might be protected by a third party DDoSM, and so on.

Table 1 qualitatively compares the maintenance costs and efforts that we see most relevant in the comparison of the EnergyShield toolkit to an equivalent installation with independent tools.

Maintenance cost type	EnergyShield toolkit	Independent tools
Remote access point	Single point	Point for each tool
Application update process	Single process	Process for each tool
Contract management	Single contract	Multiple contracts
Enterprise architecture management	Single platform with several tools (containers)	Several independent systems with own issues
Providing software updates for middleware	Partly homogenous middleware, smaller number of components, single contact for maintenance	Larger number of “random” middleware components, several contracts for maintenance
Troubleshooting	Single contact has to deal with the problem – single ticket; single process for installing bug-fixes	First, the correct tool vendor has to be identified, each tool vendor might have own ticket system / process; risk of nobody responsible for integration issues between tools; independent processes for installing bug fixes
Platform management	Costs for managing the EnergyShield platform	No platform management costs
Change management process	Single change management process	Independent change management processes
Integration tests after changes in single tool	Partly upfront integration tests on side of toolkit developers, integration	Integration tests not provided by independent tool providers – third

	tests by the customer's toolkit provider	party needed or own effort
Regular software health checks, backups, recovery test	Single process (e.g., one backup strategy for all)	Independent heterogeneous processes

Table 1: Types of maintenance costs and efforts for the toolkit / tools comparison.

To have quantitative data for the CBA and ROI, we created the estimations in Table 2 and Figure 2 based on own expectations after experiences within the project so far. Key observations are:

- For only one tool, it makes financially not much sense to choose the toolkit, because maintenance will have to cover the toolkit platform, and the tool and it would be 40% higher in maintenance than only for the tool.
- We expect that the maintenance costs and effort meet for more than three tools. This means, the maintenance costs and effort per tool are lower for the toolkit per tool than for independent tool for more than three tools.
- We expect that the maintenance costs for the independent tools will grow exponentially (e.g., for 5 tools it is with 600% more than 5x100%). The reason is that we assume that the independent tools must be integrated and this causes more and more issues with a larger number of tools. In the case of a failure, the tool vendors could try to claim that another party is responsible for a failure.

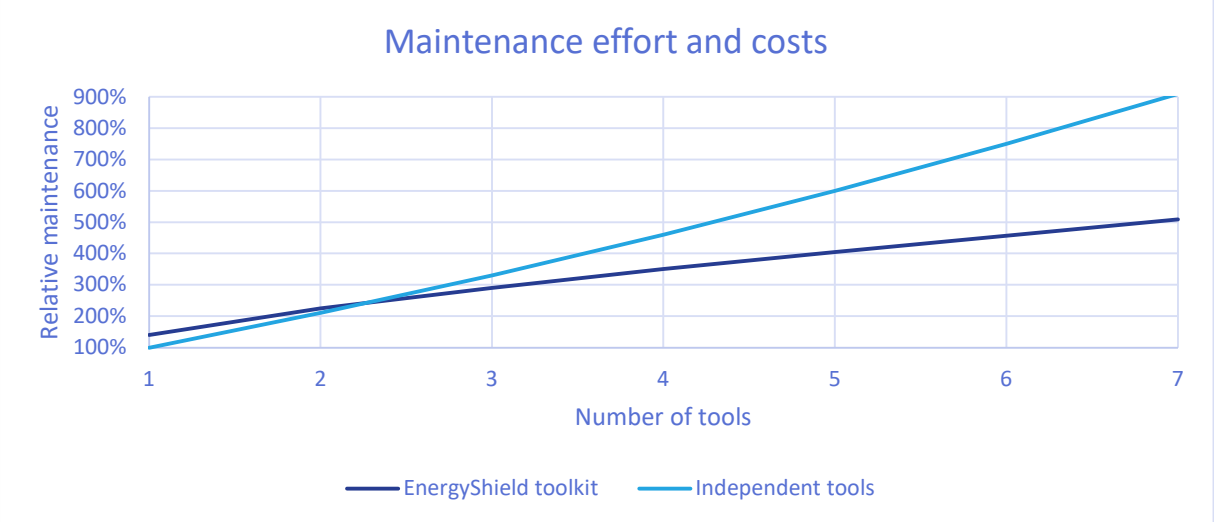

Figure 2 Maintenance effort and costs of the EnergyShield toolkit compared to independent tools.

Number of tools	EnergyShield toolkit	(Delta)	Independent tools	Difference
1	140%	+140%	100%	-40%
2	225%	+85%	210%	-15%
3	290%	+65%	330%	+40%

4	350%	+60%	460%	+110%
5	405%	+55%	600%	+195%
6	457%	+52%	750%	+293%
7	509%	+52%	910%	+401%

Table 2: Maintenance cost assumptions corresponding to Figure 2.

3.2.2. IMPROVED SECURITY FROM INTEGRATED TOOLS

We estimate that the integrated toolkit will provide 5-100% (average 15%) better overall security compared to isolated tools. The estimate is based on general expectations / educated guesses from several project partners collected by a survey. The expectations were collected recently so it includes some experience (not measurements) from the field trials.

3.2.3. PRICE DISCOUNT FROM A TOOLKIT

The EnergyShield toolkit could be sold for a price below the total sum of several comparable tools independently because of several reasons, such as the synergies in the sales process: A good sales-person could sell several tools of a toolkit within a single sales process or even with a single contract that just has a table with all the tools to select from. However, not necessarily a price reduction is justified, because the customer will also save resources from having a single larger purchase process instead of multiple smaller purchase processes (see 3.2.1.1).

Since cybersecurity products are complex products that must be explained, the sales process is not trivial, and savings in sales can be a larger part of the total transaction. Additionally, the number of meetings for the customer to make the purchase decision might be lower and the people involved in making the decisions to purchase the tools might be similar in many (but not all) cases. Especially attendees from IT, security, and purchasing departments might always be part of this.

3.3. BENEFITS IN TERMS OF REDUCED RISKS

In the following the very typical costs risks are characterized for DSOs, TSOs, and GenCos in the European energy sector. Only very typical characteristics are discussed. The national regulation in every country regarding which customer data an energy company has, and the companies have individual freedom in implementing or not following particular business models. For instance, in some countries, DSOs might collect detailed energy consumption measurements while this is untypical in other countries. Some EU countries allow smaller utilities to be both a DSOs and a retailer/supplier, which involves having more potentially GDPR-related data records than just required for DSO business.

3.3.1. IMPACT AND COST FOR ENERGY COMPANIES

In the following the impact and costs on the energy company that was victim of a cyberattack are analyzed. The focus is on grid operators and some aspects of generation companies and retailers/suppliers are discussed as well.

3.3.1.1. POWER OUTAGES

Across Europe exist different regulations for grid operators to compensate customers for power outages. Different national regulations seem to vary from no compensation, compensation after legal case, and to automatic compensation. Some different regulations from different countries are summarized in the following:

- In Italy, grid operators must compensate LV private customers if the duration of the outage exceeds 8 hours. Instead, Grid operators must compensate MV private customers if the duration of the outage exceeds 4 hours and/or if number of temporary power outages greater than 7. These SAIDI and SAIFI limits, both for LV and MV, are set by the regulator (ARERA).
- In Greece, grid operators seem usually to reject compensations for power outages caused by exceptional events such as extreme weather. However, in the case of up to 70.000 household without electricity caused by snow in Athens earlier in 2021, some power companies compensated customers with discounts on the customers' bills, as reported in [KTG21].
- The British grid operator UK Power Network describes the national compensation rules in [UPN20]. For instance, for outages the following rule applies: "If your electricity supply fails [… and …] it takes us more than 12-hours from the time we are made aware of the loss of supply, we will pay you £75 if you are a domestic customer and £150 if you are a business customer. We will pay another £35 for each additional 12-hours you are without supply."
- The German power grid regulation (NAV §18, https://www.gesetze-im-internet.de/nav/__18.html) defines low voltages liability rules upon which claims can be made for proven losses. The regulation defines conditions, total liability limits, and liability limits per customer. There is no liability for extreme-weather-like scenarios. Extreme weather is at least in the German transmission grid the primary cause of outages according to [BBR18]. For a legal case on liability for damages caused by an outage that resulted from a cyberattack, it might be relevant whether the cyberattack can be considered a "Force Majeure". A liability claim might be rejected in the case of "Force Majeure" (compare [HCS22]). In Germany, energy suppliers/retailers cannot be sued by customers in case of unplanned power grid outages. Even if a grid operator must reimburse customers for losses, the grid operator might have its own insurance to avoid own significant losses (e.g., see this report from a German outage [MDZ12]).

Some business or household insurances cover costs from some outages (for instance, here [HIQ21]). In that case, the customers might tend to avoid take the risk to sue a grid operator.

Grid operators might experience a loss of trust from their customers (and employees) after a cyberattack leads to an unplanned power outage. The value of this loss of trust would have to consider that customers usually cannot chose their grid operator. However, a mismanaged cybersecurity incident in combination with severe security weaknesses can lead to a large reputational damage and large indirect costs.

GenCos, Smaller producers, DERs (distributed energy resources), and smart buildings are not able to feed-in during a power outage, which creates a financial damage. Some but not all smart buildings are able to operate based on internal batteries and to store energy.

3.3.1.2. DATA BREACHES AND RANSOMWARE ATTACKS

Data breaches in the energy sectors that affect private households and companies can be in difference categories. Several different types of scenarios and different data types are summarized in the following:

- Customer data including bank account number, e-mail address, and contract details are stored in ERP (Enterprise resource planning) or CIS (Customer information management) systems of energy sales/retail companies. DSOs might have such data, as well for instance, for feed-in tariffs. A data breach of this data is similar to data breaches in other domains such as ecommerce.
- In some countries, grid operators or other entities store and process energy consumption details and data from AMI (Advanced Metering Infrastructure). In some cases, this data is just collected and instantly highly aggregated to allow energy retail/sales companies to perform billing, in other cases this data may be used for smart gird functionality such as load balancing or to provide customers energy consumption details in a customer portal. Some customers regard AMI data as privacy-critical because it could allow one to make conclusions about their private life [FBA14].
- Companies can have individual special contracts with their energy sales/retailers with negotiated prices or special prices or special contracts with their grid operator regarding the grid connection.
- In several countries, grid operators are required to execute feed-in-management with small renewables (photovoltaics) and the owners of the renewables get compensation in some but not all cases. It can be sensitive information which producer get how much compensation.

A data breach of the regional grid operator with stolen AMI data or private bank account data (from a non-unbundled grid operator / energy supplier) might cause stronger reactions than data breaches in other domains (e.g., social media), because a high level of trust is expected from the grid operator, and a customer has no choice

which data to publish (which is the case for social media). Additionally, in several EU countries, many grid operators are regional publicly held companies which can offer more possibilities for consequences after a data breach.

Examples for potential consequences from the data breach scenarios are for instance:

- Costs for data forensics / data recovery
- Costs for recovery (e.g., cleaning / new setup, backup recovery)
- Costs for ransom payments
- Costs from cyber shutdown
- Loss of trust and reputation
- Costs from financial loss of customers
- Fines (esp. GDPR)
- Costs for bank account monitoring
- Other legal claims

A survey by a global security company in 2021 [SSR21] determined that 32% of the victims of a ransom attack actually paid the ransom to get encrypted data back. In the energy sector the reported number slightly higher at 43% [SSR21]. The strategy "we would pay" is not a valid protection against encryption attacks – the study [SSR21] reported that only in 65% of the cases, the data was restored after paying the ransom.

Ransom demands are often adjusted to the victim's ability to pay [SSR21]. For our typical energy company, with 1.000 employees and a revenue of €1 billion, the study let us assume that a typical ransom could be a few hundred thousand euro (e.g., €200.000); however, the authors of [SSR21] point out that the ransom payments in the survey have a wide range. One recent prominent incident was the Colonial Pipeline Company attack: the company with a turnover of €1,2 billion revenue initially paid the ransom of €4,6 million [FOR21]. Therefore, it would be reasonable to consider in the risk analysis ransom demands in the range of multiple magnitudes. We assume a range of €10.000 to €10 million for our scenario.

As pointed out by [SSR21], the ransom payment is usually only one of many costs of a successful ransomware attack – the study reported a nearly nine times higher total bill for downtimes, people effort, device and network costs, and lost opportunities (average of €1,7 million).

GDPR fines

Significant fines for data breaches can result from GDPR violations. The "CMS.law" online GDPR Enforcement Tracker" [ENF22] lists publicly known GDPR fines. On 2022-03-28, 48 of the 1105 entries are from the "Transportation and Energy" sector. A closer examination of the data from [ENF22] showed that cases in the Energy Sector could be categorized into two categories:

- **Data processing failures**: Energy companies from Poland, Italy, and Romania have been issued up to seven-digit fines for GDPR violations especially in the context of advertisement and marketing in the recent years.
- **Intentional and accidental data breaches**: Several data breaches in Energy companies from Romania and Poland resulted in four-digit to seven-digit fines with stolen or disclosed data records of individuals.

As pointed out in the GDPR studies, such as the "DLA Piper GDPR fines and data breach survey: January 2022" [DLA22], the total of GDPR fines strongly increased (sevenfold) in 2021 compared to earlier years.

TSOs and GenCos usually have smaller GDPR-related risks from data breaches compared to DSOs and energy suppliers. Some TSO might have few sensors and actors in low voltage grids to fulfil the system responsibility, but the number of data records of single individuals should be limited compared to a DSO or energy supplier. Classical GenCos do not have B2C contracts and have only little privacy related data. However, a generation company might be an aggregator of many small DERs installed in private households.

3.3.1.3. POWER PRODUCTION SHUTDOWN

For a power generation company, an attack to the OT-system of can lead to a shutdown of the production process. This can cause following costs additionally to the costs from the previous section:

- Reduced delivery, sales, and revenues. A financial loss is likely, because some operational costs cannot be shut down instantly.
- Contractual penalties

Contractual penalties can occur if a power generation company fails to deliver in the context of primary reserve, i.e., failing to provide promised frequency containment tools for transmission grid operators.

Even attacks against the IT-systems of a power generation company can lead to the decision to shut down OT and production systems as well, because:

- It might be unknown, whether an attack against IT infected the OT system. This could lead to the decision to immediately shut down OT as well.
- An immediate shut down of all systems could prevent that an attack spreads to uninfected systems, that additional data is stolen or encrypted, and that forensic data is deleted

IT systems such as billing systems might not work and it might not be possible to charge customers for their power, so the management might decide to shut down the power production. Especially in the energy sector, customers might have good chances to reject energy bills if the billing system might have been hacked.

3.3.2. IMPACT AND COST FOR THE GENERAL PUBLIC

In the following, the consequences of data breaches or electrical power outages are analyzed from the perspective of the general public. The focus is on companies and private households that are customers of a grid operator or of an energy sales/retailer that suffered a cyberattack. Electrical power outages and data breaches are distinguished. Electrical power outages are covered in more detail because this is more specific for the energy sector, while data breaches are more comparable to data breaches in other domains.

A quantitative evaluation of all consequence to the public as result of cyberattacks to energy companies are out of scope of this reports. However, we identify the impact and potential categories of costs in the following.

3.3.2.1. COST OF POWER OUTAGES TO THE PUBLIC

Successful cyberattacks to distribution or transmission grid operators could cause public power outages, as proven by the cyberattacks in Ukraine 2015 and 2016 [WIR16]. Power outages can have serious impact to the health and as well as large material damage to the general public [TAB10]. The impact and costs of a power outage especially correlates to the area (street, village, city, country, EU) and time duration (minutes, hours, days, weeks …). Short power outages in small areas are not uncommon; events with more than 100.000 households affected are rare in Europe. For instance, the consequences of a long and large area power outage were in detail analyzed in [TAB10] on behalf of the Office of Technology Assessment at the German Bundestag.

In the following, some examples for consequences from regional power outages with a duration of several hours are listed:

1. Examples for potential health impact
    a. The medical treatment in hospitals has usually a limited amount of emergency power, which needs to be refilled, for instance, after one day of operation [TAB10]. Intensive care units require power to critical devices, such as heart-lung-machines operational. Even during shorter outages, it can happen that emergency power in hospitals is interrupted, as during a 2019 power outage in Berlin [BBK17].
    b. Some medical equipment outside of hospitals relies on electricity, such as dialysis devices or lung ventilators in private households or nursing homes [BBK17]. Patients might not be able to call for help, due to a lack of communication infrastructure during a power outage.
    c. Numerous accidents with injuries and fatalities can occur [TAB10] because of traffic lights outages.
    d. After a short period, public water supply will fail because of inactive water pumps [TAB10]. This eventually leads to health issues.
2. Examples for damages and financial loss

a. **Loss of opportunities:** Supermarkets and other stores are more and more not able to sell products, because payment and sliding doors rely on electricity and many European supermarkets have no backup power [TAB10]. Companies could lose contracts to competitors if they cannot participate in an online-negotiation, cannot provide an offer, or miss deadlines for submitting an offer or order (e.g., in a tender).
b. **Damaged goods:** Some goods such as food or medicine require controlled temperatures. Power outages can make them worthless. For instance, the 10th largest steel production plant in Germany reported damaged goods of up to €600.000 after a power outage of three hours [SZE20].
c. **Reduced production and services:** During an outage, companies are usually not be able to produce and sell goods or provide services.
d. **Damaged production lines or facilities**: In some cases, production equipment can get damaged in case of a power outage. For instance, if a process uses hot materials that could get stuck in machines if they cool down, or processes that require constant cooling to avoid damages. For instance, some process with hot metals that can get damage to processing machines if the metal cools down within the machines.
e. **Costs for replacements**: Power outages in critical environments can be handled by emergency power generators. However, these generators are usually less efficient and there are costs for fuel or maybe for generator rental.
f. **Costs for services**: During power outages, some additional labor costs for public or private services (e.g., logistics, emergency shelters) might occur that can be a subject for compensation claims.
g. **Fees or fines:** Losses from not meeting contractual deadlines for services or deliveries.
h. **Loss of trust:** The general public and companies might lose trust in the infrastructure or in the authorities. In the long run, this can lead to companies preferring other locations, which results in fewer jobs and less wealth for the general public.

There are methods to quantify the value of better power supply (e.g., fewer or reduced impact of blackouts), such as the “Value of Lost Load (VoLL)” approach described in [JRC19] for analyzing improvements for Estonia, Portugal and the Netherlands. However, it is beyond the scope of this report and beyond our available data to quantify the relation between cybersecurity invests and the power system reliability (i.e., the outage risk). Power outage risks for certain physical grid investment decisions are well known, while nearly no data (except the Ukraine cyber incident 2015/2016) is available for cybersecurity distribution power outage risks. For a concrete energy company, the EnergyShield vulnerability analysis tool would be an

ideal way to study the impact of concrete cybersecurity investments to the risk that the OT systems get compromised.

3.3.2.2. DATA BREACH COST FOR THE PUBLIC

Data breaches (whether ransomware was involved or not) can have impacts to:

- Private customers: Bank account details, contact information can be misused for identity theft crimes and other illegal activities. A recent study [MZS21] showed that victims are especially very or extremely concerned about the exposure of the physical address. After private data is compromised, the victims can have a lot of effort to change information such as bank accounts, phone numbers, or email addresses. Identity theft can have serious mental, emotional and physical health consequences, as reported by [IER19].
- Commercial customers and institutions: Bank account details or other data could be misused, and confidential business details could be part of the contracts between companies and their grid operator or utility company.

Some quantifications on cybercrime and identity theft exists; for instance, the Australian Institute of Criminology estimated €2 billion for 2018-19 identity crime costs [AIC20] with examples of average costs per individual of €200.

3.3.2.3. POWER PRODUCTION SHUTDOWN COST TO THE PUBLIC

Attacks to power generation companies can have consequences to the public: The transmission system can get into an imbalance between generation and consumption. There are mechanisms such as primary reserve energy, which compensate failures of parties to fulfill contracts.

However, a shutdown of a generation company because of a cyber-attack during an already tense system situation could lead to a crisis in the transmission grid, which could lead in extreme cases to large area power outages (see Section 3.3.2.3).

Even if outages can be avoided, several types of costs exist (e.g., for higher short-term energy prices) that are not taken by the generation company that failed to deliver its service.

3.4. COST ITEMS OF IMPLEMENTING THE ENERGYSHIELD TOOLKIT FROM THE TOOLKIT PROVIDERS' PERSPECTIVE

Efforts and the corresponding costs of the partners that create and develop tools, and serve the customer can be a foundation for the price that a customer must pay for the toolkit and its installation. We assume a strong correlation in this case between the costs and the price, however, a pricing strategy can to some extent ignore the costs, for example, by setting the price to the value from the perspective of the customer. In

the following, typical efforts of a toolkit provider are described (internal costs of the tool providers, e.g., for tool development are excluded):

- Sales and presales: presentations, demonstrations, contract definition and legal verification, bidding, negotiation, definition of project scope, identification of hardware and required third party licenses, definition of service and maintenance, negotiation
- Specification: Identification of all implementation and integration details in a specific customer environment, functional and non-functional requirements, data integration planning, project planning
- Installation and integration: hardware setup and preparation, installation, configuration, development of integrations to the environment, project management, testing (integration test), data integration and data modelling, adaptation to national requirements or company-specific requirements
- Transfer into production operation: acceptance test, system manual delivery, user and admin training
- Maintenance and support services: Definition of process, systematic methodology and interfaces, negotiation (if not done upfront in sales), initialization, execution of support services such as for bug removal, troubleshooting, other user support, installation of updates/upgrades, definition and implementation of backup- and recovery strategies, regular health checks, data model maintenance (data updates that cannot be done by the customer himself)
- Extensions of scope: e.g., integration of additional systems, processes and users, or for the implementation of additional functionality

3.5. EXAMPLE PROJECT SCOPE

3.5.1. CUSTOMER PROFILES

For the calculation of CBA and ROI analysis two simplified example customer profiles are assumed. The idea to use a DSO of this sizes arises from a survey among the product managers of the tool providers and project internal industry experts in the context of deliverable D8.2 [ESD82], because this would provide a sufficient large number of potential customers with sufficient cyber budgets, and it would allow to reuse most of the experiences made in the field trials. From the market segment analysis in Section 4.3 on page 47, let us estimate that there are at least more than 50 DSOs larger than DSO 1 in Europe (some DSOs are much larger, many DSOs are smaller). It is assumed that 2,3 people live in each household.

	DSO1	DSO2
Company type	Electrical distribution grid operator (DSO)	
Customers (households)	1,5 million	3 million
Employees	1.000	2.000
Yearly turnover	€1 billion	€2 billion
HV/MV substations	100	200

Table 3: Example customer profiles.

3.5.2. PROJECT DIMENSION SCENARIO

The EnergyShield field trials were pilot projects – for the CBA and ROI, it is desired by EnergyShield's Grant Agreement to address a roll out scenario. This means that the project is larger in its dimension and that it has to operate in production systems. However, rollout should not be considered as a complete application of all tools into every point in the example customers. For instance, the Anomaly Detection tool has a hardware probe that each connects and converts to a handful analog signals; however, a medium-sized DSO, such as DSO1 & DSO2 in Table 3, might have hundredths of primary substations (HV/MV) and might tens of thousands of secondary substations (MV/LV). Substations can have tens, hundreds, or even thousands of measurement points, with millions of measurement points and it would be not efficient at all to equip all of these with additional hardware probes. A realistic large AD project would focus on several of the most critical substations in within these substations only at selected measurement points.

The project scenario for DSO1 is specified as follows:

- The rollout for Anomaly Detection is assumed for 6 MV/HV substations with each approx. 5-20 measurements. Even in the case of the complete failure/manipulation of the central SCADA, operators could get a reasonable feeling based on these measurements.
- DDoSM protects 3 APIs, such as those of smart metering (AMI), communication with smaller renewables, and data exchange with the regulator.
- For the VA, we assume to cover most critical points of the IT- and OT-Network (6 high value assets). Models of network and system-architecture are modeled in the VA tool, vulnerability scans are executed in three network zones, and configuration files from three sources such as firewalls are imported. Five workshop iterations with the customers IT and security teams for both the IT- and OT-network are used to identify and simulate the system model.

- For the SBA, it is assumed that the majority employees are covered (at least those with access to network/IT).
- An (initial) rollout of the SIEM would cover 30 major IT- and OT-systems/applications of the more than 100+ central applications a typical DSO might have. For simplicity PCs or laptops are not included. For each application, there is at least an integration of log-files (e.g., login failures) and instrumentation with probes (e.g., health checks). The SIEM will have customized dashboards and correlations that integrate the single information into a complete picture.

DSO2 would have a relatively similar project specification. A major difference would be that DSO2 has more employees to address with the SBA. However, to some extent the SBA scales well with the larger company size of DSO2 because the structures of DSO1 and DSO2 can have a quite similar structure with just different numbers of teams for a certain purpose. Some license costs and tool installations would be to some extent larger for instance, to serve a larger number of users or to deal with more information to be processed – however, the general system landscape can be similar, because the duties of both companies can be equivalent. Several aspects would be the same for DSO2, such as the number of APIs monitored, and the number of substations covered by AD in the first step. The VA would be relatively comparable, because the system landscape architecture could be relatively identical for both companies (only more powerful hardware because of more users, processes, volumes, data records).

3.5.3. PROJECT PRICE EXAMPLE CALULATION

In previous EnergyShield work [ESD82], we identified an example business model and an example price model to study the toolkits exploitation strategy. In Table Table 4, we provide a simplified example project price calculation for the purpose of the CBA and ROI computation. It is called an example calculation, because business internals of the toolkit are not visible, not shown, simplified, and other aspects are still subject to negotiation and discussion between project partners. Some input prices have both been discussed with toolkit providers and end users (i.e., energy companies) of the project.

Ps.	Description	DSO1	DSO2
1	Price tool specification / installation / test	282.500 €	329.625 €
2	Reduction due to toolkit platform project	- 45.200 €	- 52.740 €
3	Price 0	237.300 €	276.885 €
4	Initial platform setup price	23.833 €	42.167 €
5	Integration costs for 5 tools	60.000 €	60.000 €
6	Price 1	321.133 €	379.052 €
7	Tool licenses (1st year)	167.500 €	254.523 €
8	Price 2	488.633 €	633.575 €

9	Quality management (5% of price 0)	11.865 €	13.844 €
10	Central project management (10% of price 0)	23.730 €	27.689 €
11	Sales costs (5% of price 0)	11.865 €	13.844 €
12	General contractor risk (3% of price 0)	7.119 €	8.307 €
13	Price 3	543.212 €	697.258 €
14	ES central platform development (5% of price 0)	11.865 €	13.844 €
15	ES central marketing (5% of price 0)	11.865 €	13.844 €
16	Intel. Property and other costs (5% of price 4)	29.839 €	38.155 €
17	**Price 4 - Contractual project price for the customer**	**596.781 €**	**763.102 €**

Table 4: Price calculation example for the initial project for the first year.

Additional information on Table 4:

- Positions (9-12) correspond to project activities of the general contractor.
- Positions (14-15) contribute to central activities of EnergyShield.
- Positions 3, 6, 8, and 13 are subtotals of the other positions, position 17 would be the total price the customer would pay to the general contractor.

3.5.4. MAINTENANCE AND SERVICE CONTRACT PRICE EXAMPLE

An example price calculations for the maintenance and service contracts is presented Table 5. It follows a similar simplified structure as described in the previous section for the initial project.

Tool maintenance price reductions of 16% (in average over all tools) are expected from the platform. These reductions are for example result from synergies in shared remote maintenance and a known execution environment. It should be noted that the operation and maintenance cost reduction mentioned in the last section are higher than this number because the previous section is about the complete customer's perspective including the customer's internal hidden costs. Additionally, costs are not equal to prices.

Pos.	Description	DSO1	DSO2
1	Maintenance execution price tools	41.000 €	50.050 €
2	Reduced maint. costs from platform	- 6.560 €	- 8.008 €
3	Maintenance price 0 (mp0)	34.440 €	42.042 €
4	Platform maintenance	16.767 €	20.433 €
5	Maintenance price 1	51.207 €	62.475 €
6	Tools yearly license	167.000 €	254.523 €
7	Maintenance price 2	218.207 €	316.998 €
8	Quality management (5% of mp0)	1.722 €	1.722 €
9	Central project management (5% of mp0)	1.722 €	1.722 €

10	Sales costs (2% of price 0)	689 €	1.722 €
11	General contractor risk (3% of mp0)	1.033 €	1.033 €
12	Maintenance price 3	223.373 €	323.198 €
13	ES central platform dev. (5% of mp0)	1.722 €	1.722 €
14	ES central marketing (5% of mp0)	1.722 €	1.722 €
15	Intel. property and other costs (5% of mp4)	11.938 €	17.192 €
16	**Maintenance price 4**	**238.754 €**	**343.833 €**

Table 5: Example maintenance and service contract price from the customer.

3.6. ROI COMPUTATION (INCLUDING EVALUATION OF CBA)

The Return-on-investment (ROI) is a traditional KPI that has been used since centuries [PPP08]. Many companies put ROI calculations as relation between the profit and the invested capital in their public annual reports. ROI calculations might differ in terms of including or ignoring positions such as taxes and interest for the company capital. As pointed out by [PPP19], "ROI is about 'value for money'" [PPP19] and goes usually beyond financial return on investment. Moreover, it is "determined by stakeholders' perspectives, which may include organizational, spiritual, personal, and social values". In this document, both a financial ROI will be presented, and additional non-financial values will be discussed.

Both ROI and CBA are related, because ROI calculations can be accomplished based on cost-benefit analysis [PPP19]. For both the ROI and the CBA, both costs and benefits are identified and quantified.

A cost-benefit analysis (CBA) is in its basic notion the comparison of costs and benefits of a particular issue, such as a project, to make a decision whether to do the project or not [LGL94]. Our cost-benefit analysis question is from the perspective of the energy sector company: Should the company start roll-out implementation project of the EnergyShield toolkit or not. Therefore, the alternative to starting the toolkit project is to do nothing and to deal with higher security risks. As described in [PPP19] and apparent from the ROI equation below, the quantitative costs and benefits are already quantitatively compared in the ROI computation, and not separate computation is needed.

For computing the financial ROI we use this equation from [PPP19]:

$$ROI_{original}(\%) = \frac{Net\ Program\ Benefits}{Program\ Costs}\ X\ 100$$

The ROI for cybersecurity products is special because it is not the primary purpose of cybersecurity invests to produce financial income. Our approach for the business value/benefit is to quantify the reduction in of risks their related financial consequences. Therefore, our equation could be rephrased like this:

$$ROI_{adapted}(\%) = \frac{Reduction\ of\ cyber\ risk\ costs - Total\ ES\ toolkit\ costs}{Total\ ES\ toolkit\ costs}\ X\ 100$$

The $ROI_{adapted}(\%)$, which will be just named ROI(%) in the remainder of this document, is above 0% if the benefits are higher than the costs. In that case the cost benefit question to implement a project would have a positive answer. A negative ROI(%) would mean that the invested capital was not returned. (For simplicity, capital costs are not modeled in this document).

3.6.1. ROI ASSUMPTIONS

In the following we compute the ROI(%) for the EnergyShield toolkit in the context of several assumptions:

- **Time horizon**: We consider the relevant time period for the ROI of 8 years - in the first years the cumulative benefit might not yet to cover the costs of the initial project. The toolkit will provide its security value much likely for a longer period than 8 years, but after 8 years, major upgrade, and hardware replacements might occur.
- **Cybersecurity attacks:** Both a ransomware data breach and an attack against the OT network with its SCADA system with a power outage are (separately) modeled. The data breach might be roughly inspired by the 2022 Fortum Poland GDPR case (fine €1 million with a beach involving the copying of data by unauthorized persons [EDP22]) and the 2020 ransomware attack on EDP Portugal (ransom demand of €10 million [OBS20]). The OT network attack was inspired to some extent by the 2015/16 Ukraine DSO cyberattacks [WIR16] with several hours blackout for more than 200.000 people. In this study, we assume 4h power outage during a business day during work hours.
- **Benefits with and without cybersecurity insurances:** Cybersecurity insurances could cover some of the risks and costs of cyberattacks. A recent Harvard Business Review article [HBR22] stated that “cyber insurance is becoming more of a must-have for business” because of increasing risks. The ROI is computed both with and without a cyber insurance to analyze financial consequences.
- **Benefits with and without considering damage to the public:** One of the leading cyber experts described the problem that the costs of bad security are often not borne by those who are responsible for it [BSB15]. The problem is described in the context of (operating system) software, but it could be the same with a DSO’s motivation for cybersecurity invests, if the public covers too much of the costs of cyber incidents. The energy sectors regulator has many existing tools to adjust this. To study this issue, both the ROIs are estimated from the financial perspective of a DSO and from the public.
- **Customer scenario** as described in Section 3.5.1: DSOs with 1,5 and 3 million household customers.

3.6.2. CYBER INCIDENT EXAMPLES

Table 6 and Table 7 show the probability and cost estimates for DSO1 and DSO2 for the first cyber-attack scenario, which assumes a data breach (DB-attack) with stolen customer records and encrypted systems. The PERT estimation method for dealing and indicating uncertainties; for instance, there might be nearly no GDPR and other fines if the corresponding national agency sees major violation on side of the company and a high number is assumed, if the data breach involved detailed data such as AMI and billing data in combination with severe data handling flaws.

	Opt.	Pess.	Real.	PERT
Yearly prob. of successful attack	5%	30%	10%	13%
GDPR and other fines	10.000 €	2.000.000 €	500.000 €	668.333 €
Customer Services	20.000 €	3.000.000 €	1.500.000 €	1.503.333 €
Recovery	50.000 €	10.000.000 €	1.000.000 €	2.341.667 €
Data forensics and consulting	50.000 €	1.000.000 €	150.000 €	275.000 €
Ransom payment	10.000 €	10.000.000 €	500.000 €	2.001.667 €
Loss of own productivity	0 €	6.000.000 €	600.000 €	1.400.000 €
Total costs (without insurance)				**8.190.000 €**
Covered by cyber & liability insurances	80%	10%	35%	38%
Total costs (with insurance)				**5.050.500 €**

Table 6: Data breach & ransomware encryption scenario for DSO1.

	Opt.	Pess.	Real.	PERT
Yearly prob. of successful attack	5%	30%	13%	15%
GDPR and other fines	10.000 €	2.000.000 €	500.000 €	668.333 €
Customer Services	20.000 €	6.000.000 €	3.000.000 €	3.003.333 €
Recovery	50.000 €	10.000.000 €	1.000.000 €	2.341.667 €
Data forensics and consulting	50.000 €	1.000.000 €	150.000 €	275.000 €
Ransom payment	10.000 €	10.000.000 €	500.000 €	2.001.667 €
Loss of own productivity	0 €	12.000.000 €	1.200.000 €	2.800.000 €
Total costs (without insurances)				**11.090.000 €**
Covered by cyber & liability insurances	80%	10%	35%	38%
Total costs (with insurances)				**6.838.833 €**

Table 7: Data breach & ransomware encryption scenario for DSO2.

In the following, some general remarks on Table 6 and Table 7 are provided. Not all values have differences between DSO1 (Table 6) and DSO2 (Table 7).

- The probability of a successful attack is slightly higher (15% instead of 13%) to adjust the fact that a twice as large DSO might be more attractive to more professional attackers.
- The GDPR fines are not distinguished for DSO1 and DSO2. However, there are some aspects such as the companies' turnover and number of customers that

have been affected by the data breach that would be larger for DSO2, which could be adjusted for better estimations.

- Customer services costs are assumed to be relative to the number of customers, which could be the case, if for instance, every customer is informed by letter.
- Recovery and data forensic costs are assumed to be quite similar for DSO1 and DSO2. However, log-files etc. of DSO2 might be larger, requiring more analysis.
- We assume approximately similar ransom demands for simplicity. The ransom of €10 million might high compared to other ransom demands in the energy sector.
- The potential loss of productivity refers especially in the pessimistic scenario that large parts of the employees cannot work efficiently for days or weeks because of ongoing new system installations and manual data retrieval in case of lost data. It is assumed to be in relation to the number of employees, and therefore larger for DSO2.
- The insurance estimates have a relatively high uncertainty as indicated in the spread between optimistic and pessimistic. A report [WTW20] indicates slightly higher rates (e.g., 44% in average paid by insurer for data breaches), but we are unsure whether that data is valid for European DSOs and these types of costs.

	Opt.	Pess.	Real.	PERT
Yearly prob. of successful attack	0,5%	5%	2%	2,25%
System recovery	1.000.000 €	20.000.000 €	4.000.000 €	6.166.667 €
Private customer compensation	0 €	3.000.000 €	1.500.000 €	1.500.000 €
Commercial customer comp.	100.000 €	3.000.000 €	1.500.000 €	1.516.667 €
Data forensics and consulting	100.000 €	1.500.000 €	250.000 €	433.333 €
Damaged OT equipment	0 €	5.000.000 €	400.000 €	1.100.000 €
GDPR and other fines	5.000 €	500.000 €	20.000 €	97.500 €
Loss of own productivity	0 €	7.500.000 €	600.000 €	1.650.000 €
Total costs				**12.464.167 €**
Covered by cyber & liability insur.	80%	10%	30%	35%
Non-insured costs				**8.101.708 €**

Table 8: 4h power outage from an OT cyber-attack for DSO1.

	Opt.	Pess.	Real.	PERT
Yearly prob. of successful attack	2,0%	8%	3,5%	4,00%
System recovery	1.000.000 €	20.000.000 €	4.000.000 €	6.166.667 €
Private customer compensation	0 €	6.000.000 €	3.000.000 €	3.000.000 €
Commercial customer comp.	200.000 €	4.500.000 €	2.250.000 €	2.283.333 €
Data forensics and consulting	100.000 €	1.500.000 €	250.000 €	433.333 €
Damaged OT equipment	0 €	5.000.000 €	400.000 €	1.100.000 €
GDPR and other fines	5.000 €	500.000 €	20.000 €	97.500 €

Loss of own productivity	0 €	15.000.000 €	1.200.000 €	3.300.000 €
Total costs				**16.380.833 €**
Covered by cyber & liability insur.	80%	10%	30%	35%
Non-insured costs				**10.647.542 €**

Table 9: 4h power outage from an OT cyber-attack for DSO2.

Table 8 and Table 9 show the probability and cost estimates for DSO1 and DSO2 for the second cyber-attack scenario, which assumes that the OT systems are compromised (OT-attack) and used to cause an unplanned power outage in the DSOs grid. Only some positions differentiate between DSO1 and DSO2. General assumptions on Table 8 and Table 9 are:

- The yearly probability for an OT attack followed by a power outage is set lower than the probability for a successful data breach. This confirms to the limited past observations in Europe so far – there have been more ransomware attack than reported or successful attempts to shut down power grids. A probability of 2,25% could be understood “as to be expected every 44 years”. For the larger DSO2, we assume a slightly higher probability of 4% because it might be more attractive to attackers that are interested to cause much damage.
- The costs of system recovery can be very high because some OT equipment might have to be completely replace. Past OT attacks have replaced firmware of distributed field devices. OT system replacement is often more complicated than the replacement of business software because OT systems have real-time and high-availability requirements and a higher degree of specialization.
- Power outages can lead to compensation payments (see 3.3.1.1) depending on the duration and national regulation. In many EU countries, we expect small compensation payments to private households for an outage of 4 hours. The “realistic” value is set to 1 € per household, which could be a voluntary compensation payment that would cover the network fees for the fraction of a month. Some commercial customers might be successful individual lawsuits or out-of-court settlements.
- Attackers might try to damage OT equipment such as breakers or transformers. The number in the tables reflect a low expectation for damages in the grid infrastructure because additional protection mechanisms exist.
- We expect only minor risks for GDPR fines in this attack scenario, because these types of attacks are usually not related to privacy related data theft.
- The loss of own productivity can result from manual grid operations followed an attack against OT system over some period of weeks.

3.6.3. CYBER ATTACK COSTS REDUCTION FROM THE TOOLKIT

In the previous section the risk and costs of two types of cyber-attacks were quantified. This numbers can be multiplied to have risk-weighted costs or risk costs that we can used in the ROI.

Next, a central point in the CBA and ROI is an estimate how much the risk or impact of a cyber-attack is reduced from using the toolkit. The risks and costs presented in the previous section are only reduced by the toolkit – not removed. The PERT estimate for the risk reduction is shown in Table 10. The numbers are identical for both scenarios and the spread between optimistic and pessimistic estimates are quite large, which indicates both a high level of uncertainty. The available field trial measurements do not provide numbers that can be used for this estimate. After some internal discussions, we assume that PERT values of 35% are not too high.

	Opt.	Pess.	Real.	PERT
Risk reduction from toolkit for the successful data breach scenario (DB-scenario)	60%	15%	33%	35%
Risk reduction from the toolkit for the attacked followed by a power outage (OT-attack)	60%	15%	33%	35%

Table 10: Estimated risk reduction from the toolkit.

Table 11 combines the values of Table 6 to 9 and computes the risks costs weighted by the probability of a successful attack and by the risk reduction assumption, we will continue to present number with and without insurance. The two attack scenarios are combined because both risks are assumed to apply independently.

Position 9 of Table 10 shows that the EnergyShield toolkit provides every year a value of 471 K€ for DSO1 and 634 K€ for DSO2 if the DSOs have no insurances that cover the costs listed in the scenarios. Position 16 of Table 10 shows the corresponding yearly toolkit values of 295 K€ for DSO1 and 397 K€ for DSO2 if cyber and liability insurances are in place to cover some share of the costs.

Pos.	Description	DSO1	DSO2
Without cybersec & liability insurances covering parts of the risks			
1	Risk costs DB-scenario	8.190.000 €	11.090.000 €
2	Yearly probability DB-scenario	13%	15%
3	Weighted risk costs DB-scenario	1.064.700 €	1.663.500 €
4	Risk costs OT-scenario	12.464.167 €	16.380.833 €
5	Yearly probability OT-scenario	2,25%	4,00%
6	Weighted risk costs OT-scenario	280.444 €	655.233 €
7	Weighted risk costs both scenarios	1.345.144 €	2.318.733 €
8	Relative risk reduction from toolkit	35%	35%
9	**Risk reduction benefit from toolkit (yearly)**	**470.800 €**	**811.557 €**
With cybersec & liability insurance covering parts of the risks			

10	Covered by insurance - DB-scenario	38%	38%
11	Weighted risk costs DB-scenario after insurance	660.114 €	1.031.370 €
12	Covered by insurance - OT-scenario	35%	35%
13	Weighted risk costs OT-scenario after insurance	182.288 €	425.902 €
14	Weighted risk costs both scenarios after insur.	842.402 €	1.457.272 €
15	Relative risk reduction from toolkit	35%	35%
16	**Insured risk reduction benefit from toolkit (yearly)**	**294.841 €**	**510.045 €**

Table 11: Quantified yearly benefit of the EnergyShield toolkit.

At this point it is clearly visible that a cyber insurance can reduce the quantitative value (i.e., benefit) provided by a security tool and the chances for a tool to win a cost-benefit analysis and to provide a good ROI. In other cases, cyber security insurances might enforce better cyber security through contractual requirements.

3.6.4. INPUT COSTS AND BENEFITS & ROI COMPUTATION

Table 12 summarizes some input data for the ROI(%) computation. There will be 4 ROIs computed from the data in this table: with and without insurances (R1 and R2), and both for DSO1 and DSO2. The table compares costs and benefits and can therefore be considered a cost benefit comparison. First the costs and benefits for the assumed program lifetime have to be cumulated. As mentioned in 3.6.1, we assume a lifetime of 8 years. Position 3 of Table 12 list the total costs for the first year and position 6 the yearly costs for year 2 to 8.

The “hidden costs” (Pos. 2 and 4) corresponds primarily to effort on the side of the customer to maintain and manage the system and related support processes. Especially a SIEM system is usually adapted to changes in the infrastructure that is monitored from time to time. (See 3.2.1 or [HLA03] for more on “hidden costs”).

Pos	Description	DSO1	DSO2
Costs (i.e., investment)			
1	Toolkit implementation project contract price (year 1)	596.781 €	763.102 €
2	Hidden project implementation costs of customer (year 1)	397.854 €	508.735 €
3	Total internal and external costs year 1	994.636 €	1.271.836 €
4	Maint., service, license contract price (year 2..8)	238.754 €	343.833 €
5	Hidden maint. & service costs of customer (year 2..8)	179.066 €	227.414 €
6	Total yearly internal and external costs year 2..8	417.820 €	571.247 €
Benefits (i.e., value)			
7	R1 - Without insurances: risk reduction benefit (year 1..8)	470.800 €	811.557 €
8	R2 - With insurances: risk reduction benefit (year 1..8)	294.841 €	510.045 €

Table 12: Input data for the ROI computation.

The result from the computation of the ROI(%) is shown in Figure 3, the ROI(%) data behind the visualization is in Table 12 in Appendix C – ROI-Table at the end of this document.

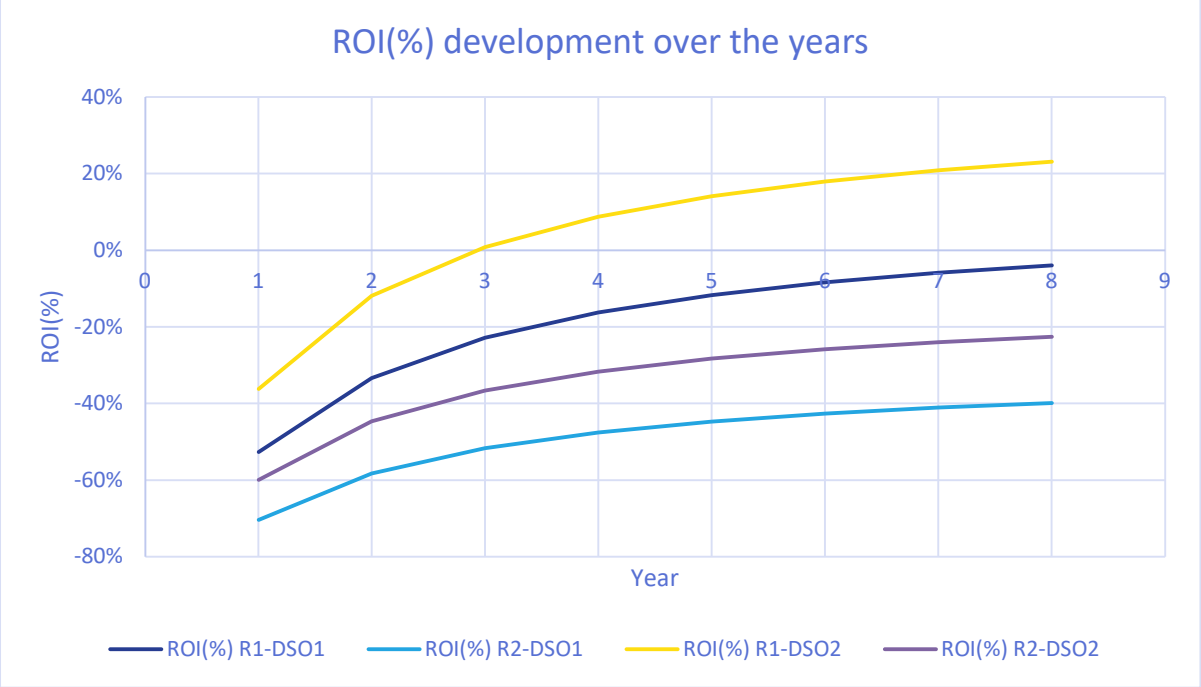

Figure 3: ROI(%) Results for DSO1 and DSO2 with and without insurances.

Both DSO1-ROIs (i.e., with and without insurance) and the R2-DSO2 (i.e., with insurance) are negative over the complete time horizon of 8 years. This means that the toolkit financial costs are not covered by the value resulting from the reduction of the risks.

Only the ROI-DSO2 is positive after 4 years and more years. This is the larger of the two DSOs and in the case of R2, there is no insurance that covers 38% of the costs of the risks.

It is clearly visible that cyber insurances have a negative impact on the ROI of the EnergyShield toolkit – the R1 variants are for both DSO1 and DSO2 much better than the R2 variants.

DSO1 is already a large company with 1000 employees and 1,5 million households supplied via the company's distribution gird. Still the investment of a toolkit that provides in our assumptions a good reduction of the risk of cyber-attacks would not be taken from the perspective of this pure financial analysis.

For DSO2 it, would make sense to invest into the toolkit, but only if the risks are not already covered by a cyber insurance.

It could be argued that a major problem exists in the fact that costs to the public only are not assigned to the company that could significantly reduce the risks with means such as installing the EnergyShield toolkit. To study this issue, next the ROI(%) is

computed if some of the costs to the public of the data breach risk and the OT-attack / power outage risk are passed to the energy company.

3.6.5. ROI(%) WITH COSTS OF THE PUBLIC

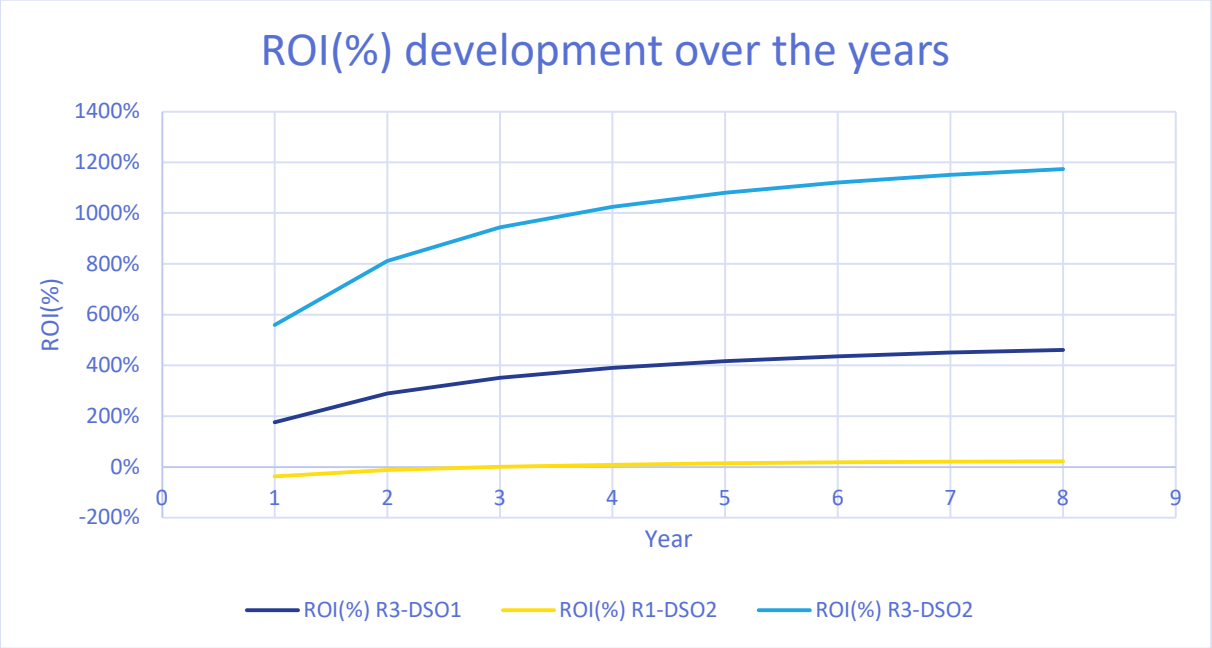

Figure 4: ROI(%) development with costs of the public considered in R3-DSO1 and for R3-DSO2.

Figure 4 introduces a new scenario R3 for DSO1 and DSO2 that additionally includes the costs of the public. To compare the chart with the previous one, the yellow scenario R1-DSO2 is shown in both diagrams. R1-DSO2 performed best in the previous evaluation (Figure 3), but in this completion, it is nearly not visible that it has a different value than 0%, because R3 leads to very high Return-on-investments, right from the beginning. In other words, there would be a clear decision in favour for the EnergyShield toolkit if the costs to the general public would be considered (if the assumptions and estimations are considered valid). Even for the smaller DSO1, there would be a clear decision to install the EnergyShield toolkit (or equivalent alternatives)

The costs of the public from the power outage are estimated based on GDP (Gross domestic product):

- GDP per capita EU 27: 32.272€ (source: Eurostat [ENA22])
- A 4h outage duration is assumed. It is on a business day during work time. GDP loss per capita for 4h power outage during worktime: €65,33 (GDP per capita / 2 * 247 workdays; Source workdays: [ECB22])
- 1,5 million and 3 million households correspond to 3,45 million capita for DSO1, 6,9 million capita for DSO2 (source average household size 2,3: [EST21])

- Costs to the general public (GDP based estimate):
    1. DSO1: €225.381.377
    2. DSO2: €450.762.753
- It should be mentioned that this is only one simple possible perspective to estimate the costs of the public. On one hand, the actual costs might be lower, because people might just shift their work times. On the other hand, the costs of the public might be higher because other costs, such as negative health impacts, fuel costs for backup power, and activities of public services are not included.

The costs of the public of the data breach are based on studies on identity theft:

- As pointed out in 3.3.2.2, the report of [AIC20] suggests €200 average costs per individual by identity theft.
- For the customers of DSO1 and DSO2 we only assume that one identity record per household exists (this is different for other utilities such as telecommunication, internet, and streaming). Therefore, 1,5 million and 3 million potential identities are considered.
- It is assumed that only 5% of the identities are stolen and misused in the data breach scenario.
- This results in identity theft costs of €15 million for DSO1 and €30 million for DSO2.
- As for the previous scenarios, it is assumed that the EnergyShield toolkit reduces the risk by 35% and the risk probabilities of 13% and 14% for the data breach scenario.
- In this case we only quantified the identity theft costs of the public. There can be more costs of the public from the data breach, e.g., for companies that are customers of DSO1 and DSO2.

In summary, it can be stated that a rollout of the EnergyShield toolkit is not favourable for a company of the size of DSO1 and even not for larger companies such as DSO2, if larger parts of the risks are covered by cyber or liability insurances and if the regulation and the courts leave most of the costs on the side of the general public. If the DSO is accountable and has to compensate the general public for all costs of both attacks, the DSO might decide for implementing a product such as the EnergyShield toolkit and reduce the risks for the occurrence of power outages and data breaches.

4. BUSINESS CASE ANALYSIS

This section complements the joint business model for the EnergyShield toolkit derived in deliverable D8.2 [ESD82] with a quantitative analysis.

As part of the business case analysis, we show market size estimations, project approaches that would finance toolkit activities, platform development and other central activities. However, internal costs and profit numbers are not provided in this public document to not reveal business internals and to not reduce the chances in contract negotiations.

4.1. ASSUMPTIONS ON THE BUSINESS CASES

Several assumptions are made to explore business case scenarios:

- Increasing security requirements over time: It is assumed that more and more security capability and tools are required in the future. This assumption is supported by the observation that in the past, only firewalls and virus scanners might have not been seen as essential requirements in the past but seems to become more and more mandatory for critical infrastructure operators. Additionally, the security product market indicates for at least a decade a growing number and variety of products and ongoing specialization of tools. However, it might be argued that the new requirements might be in many cases only extensions of existing tools; for instance, a traditional firewall product might add intrusion detection features, or a network management tool might add SIEM functionality.
- The scenarios will have different strong changes of regulatory requirements. Not fulfilling the requirements is not considered an option for larger parts of the energy sector. Therefore, the exact value of the security functionality can be excluded from the analysis in this section (in contrast to the previous section) and the focus is on average initial project and service and maintenance contracts.
- The business cases scenario analysis is quite general but could be based on the business joint business model from deliverable D8.2 example. It models one possible scenario, where customers make contracts with a general contractor (GC) it responsible to coordinate the work that has to be done by the toolkit providers and others. Some parts such as first level support, platform development, testing, and maintenance, as well as EnergyShield toolkit marketing can be centralized activities over time that will be funded for instance, from a share of the contracts to customers or the central activities can be joint shared work by the project partners.
- The business case analysis in this section will not analyze the business cases of single tools and not analyze the business case of single EnergyShield project partners.

- We only use average project prices and average project service and maintenance contract sizes for a toolkit scenario to a larger toolkit installation like the “rollout scenario” in the previous section.

4.2. MARKET FOCUS

In order to estimate the potential market for the EnergyShield toolkit, the following assumptions are made, and focus is set. A focus is set, because the complete European energy sector is quite large but it is more realistic to find customers in a market segment where our project reference and project experiences apply and where we see the best market changes. Of course, customers outside of this focus would be served as well. The focus market as subset of the European energy sector is defined as follows:

- An analysis of the most promising energy sector segments in D8.2 [ESD82] indicated that especially larger energy companies are promising as starting point for the EnergyShield toolkit. Based on the available data, the focus was set on energy sector companies with more than 250 employees with the ideal customer size of 1000 employees.
- The EnergyShield project partner companies are from different EU countries, from UK and Israel. EU market statistics do not include the UK anymore, and Israel is not part of EU market statistics. Since the UK is a large market, and older compatible EU statistics data is available, we estimate current numbers for EU27+UK. Some project partners are from Israel. Israel is included in a simplified way by only considering Israel’s national electricity utility, which still dominates generation, transmission, and distribution to a large share [MEI21] – a closer market data analysis and transformation to match EU data statistic segmentation not be efficient in provide new insights related to the business case.
- The focus of the field trials and of the project partners in the project was on generation, distribution, and transmission of electrical energy. To have get most out of the field trials as references and to maximize the benefit from experiences made in the project, therefore the focus is on electrical energy. The market segment of energy suppliers/retailers is included because of two reasons: firstly, many European distribution or generation companies are part of larger companies that are active in multiple market roles via subsidiaries, which is allowed in some European countries. Secondly, more data is available for segment D35.1 (classification D35.1 NACE Rev. 2, matching to UN segment Division 35 Class 3510 “Electric power generation, transmission, and distribution” [UNa08]) than for subsegments of D35.1.

4.3. ESTIMATION OF MARKET SIZE

Table 13 shows in the yellow-colored final row the estimated market size, while the other rows show computation steps. The details on the data source (Eurostat and DG

Energy) and the raw data is in Section 8 (Appendix Socio-economic data). The regions are distinguished between EU-27 (the current European Union member states), IL for Israel, and UK for United Kingdom. The segments refer to economic classifications (see Section 8 for details) – D35.1 corresponds to the segment "Electric power generation, transmission and distribution" which includes trading and electrical energy resellers/suppliers.

Table 13 provides several insights on the target market at this point:

- 558 companies of the many more companies in the energy sector are large companies that we consider the most likely first customers of the EnergyShield toolkit. It should be kept in mind, that there is a large difference of size within this group of 558 - some energy companies have tens of thousands of employees.
- More than 807.000 employees are in the EU/UK/IL electrical energy sector are within companies of more than 249 employees. This is especially a relevant for EnergyShield's SBA tool which focuses on the human factor in cybersecurity.
- The 558 companies have a total turnover of more than €910 billion. However, since energy trading companies are part of the segment DG35.1, turnover values can be relatively high and misleading.

Year	Company size	Region	Segment	Number of companies	Employees	Turnover (Mio €)
Computation 1: EU-only => EU+UK						
2018	*	EU-27	DG35	163.889	1.299.157	1.448.366
2018	*	EU-27 + UK	DG35	169.431	1.452.244	1.588.940
Computation 2: 2018 => 2019						
2019	*	EU-27	DG35	173.000	1.300.000	1.470.000
2019	*	EU-27 + UK	DG35	178.850	1.453.186	1.612.674
Computation 3: Only companies larger than 250 employees						
2018	>= 250 empl.	EU-27	DG35	540	909.092	-
2018	>= 250 empl.	EU-27 + UK	DG35	577	1.032.910	-
2019	>= 250 empl.	EU-27	DG35	560	923.115	1.013.502
2019	>= 250 empl.	EU-27 + UK	DG35	598	1.048.843	1.130.135
Computation 4: Only segment D35.1						
2019	*	EU-27	DG35	162.989	1.379.747	1.456.779
2019	*	EU-27	DG35.**1**	151.605	1.045.051	1.165.231
2019	>= 250 empl.	EU-27+UK	DG35.**1**	557	794.417	903.959
Computation 5: With Israel						
2019	>= 250 empl.	EU-27+UK+IL	DG35.1	558	807.093	910.359

Table 13: Estimated market size for the EnergyShield toolkit.

4.4. ANALYSIS OF BUSINESS CASE SCENARIOS

In the following, we discuss three business scenarios for the selected target energy sector segment and the financial consequences on the expected number of new projects per year and the financial consequences based on assumed average prices for the initial project for each customer and the service and maintenance contracts.

Scenario A – Acceptance of consequences instead of addressing risks:

- In scenario A most energy sector companies follow a minimalistic approach on security with little intrinsic and extrinsic pressure to improve their cyber security
- Little additional or only slow additional regulation; liability and compensation rules stay the same.
- The likelihood of scenario A would increase if no significant incidents occur in the energy sectors within the next years.
- Scenario A results in very slow linear growth adoption of sales for the EnergyShield toolkit to security affine individuals and early adopters
- No really large rollouts expected for scenario A.

Scenario B - Steady increase in security pressure:

- Additional regulatory and legal pressure for instance, driven by several big cyber incidents in the energy sector. This includes additional financial liability and compensation duties for data breaches or power outages.
- However, companies follow to prefer the cheapest product because of little intrinsic motivation of their own. Maybe some more intrinsic motivation for security invests in OT.
- One market reaction to more regulatory requirements and higher liability might the outsourcing of many functions. This might be easier to implement for IT topics and IT infrastructure monitoring (e.g., SIEM, device management).

Scenario C – Strong and continuous increase in pressure for improving security:

- Very strong additional regulatory and legal pressure with increased potential for consequences under criminal law for IT security management roles or severe financial consequences in case of cyber security implementation failures
- This scenario is likely if significant incidents occur with very high damage to the general public.
- There might be some undesired market changes, such as strong outsourcing of processes and risks. Additionally, it might be a strong decrease in small and medium-sized energy companies, because only large companies might be able to

deal with the high requirements (e.g., operating an own 24/7 SOC is too expensive for small companies).

Table 14 and Figure 5 show our estimates for the potential success for finding new customers for the EnergyShield toolkit for the three scenarios based on the experience and discussions between several product managers. Table 15 and Figure 8 show the revenue resulting from the business cases.

For scenario A it could be challenging to continuously motivate ongoing cooperation between many partners and to finance the required activities for development and marketing.

Scenario C shows a very strong growth, which would be good from one perspective. However, this might lead to a bottleneck in qualified employees to implement all the projects – EnergyShield might have synergies that reduce the efforts on the side of the supplier, but still many workshops and customer-specific efforts are required and need to be staffed with skilled experts.

Scenario B is less favorable in terms of the number of customers and business, but it might be more realistic in terms of building the capability to successfully deliver and operate the toolkit. Therefore, scenario B might even have a better profit than scenario C, because projects can be properly executed and better customer satisfaction.

As in other software markets, in scenarios B and C, preference is given to providers who can deliver comprehensive solutions for the most diverse aspects of the task. In such a scenario, providers of singular solutions will come under increasing pressure. In such an environment, the role of the manufacturer is increasingly changing from that of a supplier to that of a solution partner.

Maybe the ongoing changes in the regulatory frameworks, such as NIS 2 directive and their corresponding national implementations, and the awareness for increasing risks from international tensions and growing cybercrime are currently in favor for scenario B.

Scenario	2023	2024	2025	2026	2027	2028	2029	2030
A	0,5	1	1,5	2	2,5	3	3,5	4
B	1	2	8	16	18	19	35	36
C	2	3	14	25	38	57	62	47

Table 14: Number of new customers per year

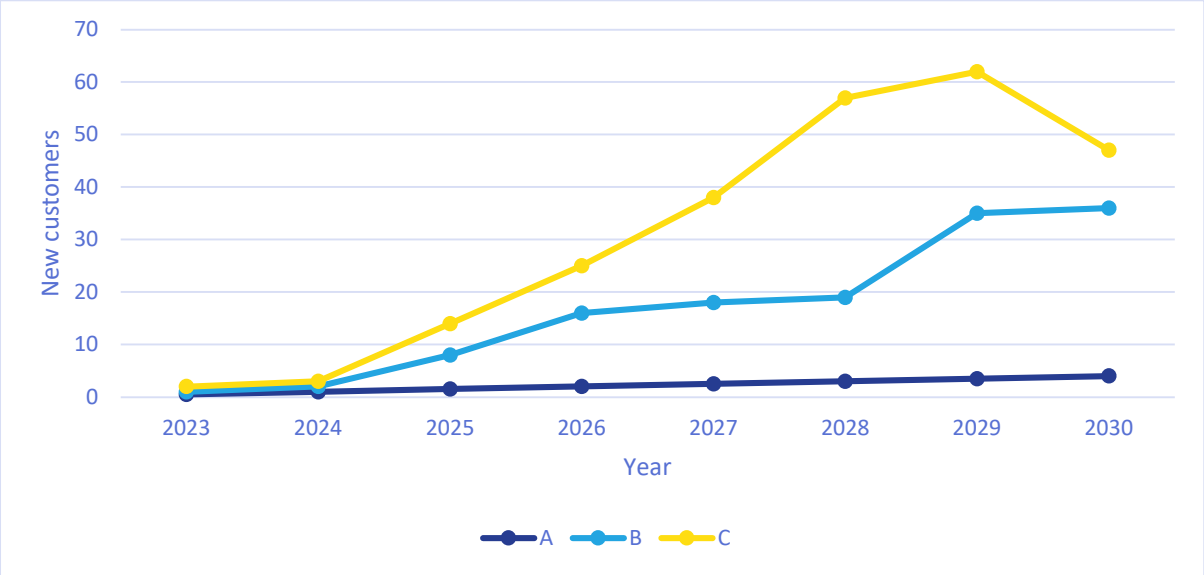

Figure 5: Number of new customers per year per scenario.

Sc.	2023	2024	2025	2026	2027	2028	2029	2030
A	0,3 Mio €	0,7 Mio €	1,3 Mio €	1,9 Mio €	2,7 Mio €	3,6 Mio €	4,6 Mio €	5,7 Mio €
B	0,6 Mio €	1,4 Mio €	5,5 Mio €	12,2 Mio €	17,2 Mio €	22,1 Mio €	36,2 Mio €	45,2 Mio €
C	1,2 Mio €	2,3 Mio €	9,6 Mio €	19,5 Mio €	33,2 Mio €	53,6 Mio €	70,2 Mio €	76,1 Mio €

Table 15: Sales from new customers and from service/license/maintenance contracts per year per scenario.

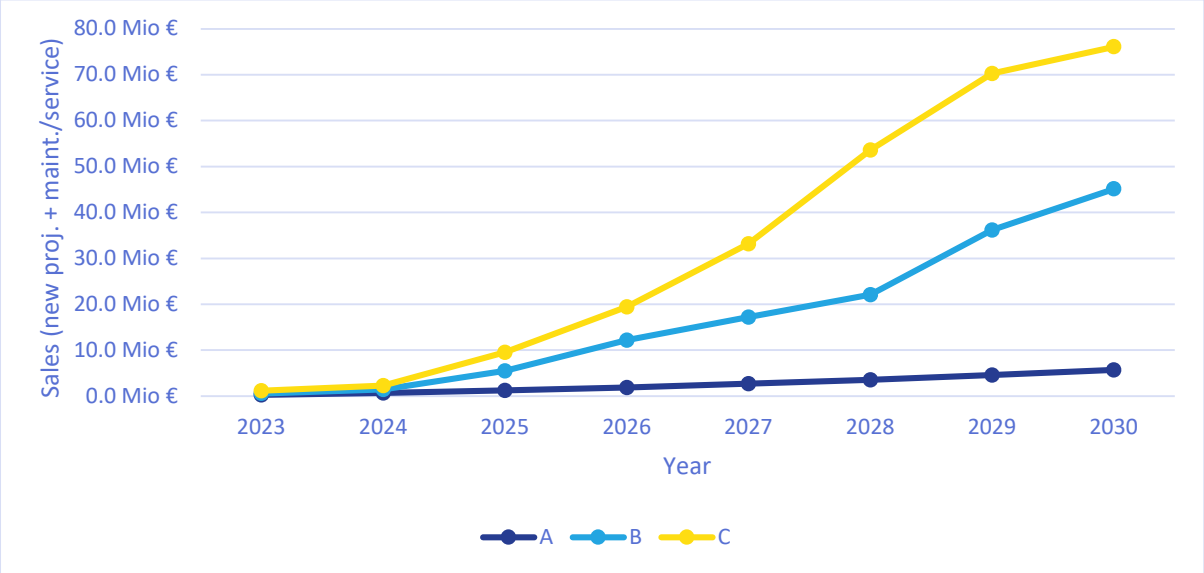

Table 16: Sales from new customers and from service/license/maintenance contracts per year per scenario.

5. SUMMARY & NEXT STEPS

5.1. SUMMARY

This report described costs and benefits of the EnergyShield toolkit both from a customer's and a toolkit provider's perspective. The focus is on the quantitative value from the customer's point of view. This value is a critical part of the previously started business model canvas. Experiences from the toolkit instantiations in the field trials and literature research were used to conduct a cost and benefit analysis for a roll out of the EnergyShield toolkit.

Two cyber incident scenarios for energy companies were studied in the analysis: a data breach and an attack to OT systems that cause a regional power outage. The financial cost were quantified both for the energy sector company that suffered the cyber-attack and for the general public.

The return-on-invest analysis showed for which companies and under which assumptions the toolkit's case is positive. For instance, the larger of the two evaluated companies (a DSO with 3 million household customers) has a positive outcome and would recommend an implementation from a purely financial point of view. Many energy sector companies have an extrinsic motivation for building up cybersecurity defenses. However, under purely economic criteria, a five tool toolkit with all the features of the EnergyShield toolkit and its operational costs might be too costly for small energy sector companies. Such companies might follow the strategy to accept risks by just paying for damages instead of investing into preemptive measures that also protect the general public. Alternatively, these companies might outsource processes in the long term. At this point, the ROI analysis explored the influence of cyber insurances and liability limitations in purely financially-driven decisions. The possible strategy to treat cyber risks with curative measures that only limit the own financial consequences, can have negative consequences for the general public. However, if these consequences are partly included and cannot be fully insured or excluded by liability limitations, then even smaller energy sector companies would have a strongly positive ROI in favour for the EnergyShield toolkit.

The business case analysis included a market segment evaluation. More precisely, the size of a suitable and promising market segment for the EnergyShield toolkit within the energy sector was estimated. This showed that there are about 558 energy sector companies with more than in total 800.000 employees together in the EU and in the countries of the project partners.

Three different business case scenarios and their possible outcomes have been explored. In the pessimistic scenario, the demand in the near future for EnergyShield-toolkit-like solutions might be too small. The two other scenarios provide promising business perspectives for the EnergyShield toolkit. Results from this will influence the ongoing business case discussions.

5.2. DISCUSSION

Our ROI results show relatively small and in some cases too small financial motivation for energy sector companies to implement higher levels of cyber security. These results can be compared to insights of Bruce Schneier, a leading author and expert in the area of cyber security and cyber security economics: [BSN16] points and comments on 2013 research of S. Romanosky [SRO16] on the costs of 12.000 cyber events that the 0,4% share of estimated annual revenues is low and that no reputational damage could be identified from stock prices. [BSN16] states, the research of Romanosky supports the position that “it often makes business sense to underspend on cybersecurity and just pay the costs of breaches”. Regulators have to fix the market, such that it makes more sense for companies to deal more with cybersecurity and that currently large parts of the costs of cyberattacks are borne by other people (e.g., the public or the customers of a company) [BSN16]. A special point in the energy sector is that bad cyber security can potentially lead to large scale power outages with very high financial and health consequences.

In recent years and currently, there have been tightened regulations and activities (e.g., NIS 2.0 and RCE) that increased and will further increase financial motivations for some energy sector companies to improve their cyber security.

Some numbers used in this document are based on expectations and educated guesses of project partners, such as the security improvement by the EnergyShield toolkit against real cyber-attacks in production environments. Other calculations are under strong assumptions. This document does not aim to qualify as scientific research. As stated by [BSU16]:“It’s difficult to analyze the cost-effectiveness of different security measures […] it’s more of an art than a science. But all is not lost.” The estimates in this document will help us to study and discuss assumptions with potential customers and to finalize the exploitation strategy.

This report does not show tool-specific quantitative data on costs and benefits and provide only average numbers for the tools. However, the tools have different installation, license, maintenance and integration effort, costs and different pricing models (e.g., subscription based). Providing those number in detail would disclose business information of tool providers and potentially weaken their business chances. The focus of this document is to address the ROI, CBA and business cases of the toolkit and not to study the business cases, ROI, CBA of the project partners.

5.3. NEXT STEPS

There are still open questions and alternatives in the design of the business model of the energy shield toolkit. Some of these open points will be discussed among the project partners in the spirit of the conclusion of the field test results. Other open issues will remain open, because a major point of a business models is that it must meet the customers’ needs. Therefore, first concrete potential customers will enable the project partners to decide how to precisely serve the market needs.

It could be valuable future work within the project duration and after the EnergyShield project period to collect additional measurements and observations that helps to improve the quality of estimates and to provide more and more quantitative arguments for potential customers.

We compared three possible market scenarios with different outcomes and their assumptions. In the remaining project time, we will continue to study the market assumptions and monitor the chances of a successful business case for the EnergyShield toolkit.

At the end, the market demand will decide whether the EnergyShield project partners will implement this business case. One or two initial projects could be provided in an ad-hoc structure – providing many more projects would benefit from central roles and central platform management.

It is future work to discuss assumptions and conclusions made in this report with potential customers to further improve the understanding of the market and to improve the chances for a successful exploitation of EnergyShield.

6. REFERENCES

[AAM17] Maria Creuza Borges de Araújo, Luciana Hazin Alencar, and Caroline Maria de Miranda Mota. "Project procurement management: A structured literature review", Apr 2017, Int. Journal of Project Management, Volume 35, Issue 3, https://doi.org/10.1016/j.ijproman.2017.01.008

[AAP10] Alain April, Alain Abran, “Software maintenance management : evaluation and continuous improvement”, 2010, Hoboken, N.J: Wiley Interscience, ISBN: 9780470258033

[ACT16] Behnaz Arzani, Selim Ciraci, Boon Thau Loo, Assaf Schuster, and Geoff Outhred, “Taking the Blame Game out of Data Centers Operations with NetPoirot”, Aug 2016, Proceedings of the 2016 ACM SIGCOMM Conference (SIGCOMM'16), https://doi.org/10.1145/2934872.2934884, Last access: 2022-04-21

[AIC20] Australian Institute of Criminology, “Counting the costs of identity crime and misuse in Australia, 2018–19”, 2020, ISBN:978192530475, Available online: https://www.aic.gov.au/sites/default/files/2020-08/sr28_counting_the_costs_of_identity_crime_and_misuse_australia_2018-19.pdf, Last access: 2022-03-02

[BBK17] F. Breuer, P. Brettschneider, P. Kleist, S. Poloczek, C. Pommerenke and J. Dahmen, „Erkenntnisse aus 31 Stunden Stromausfall in Berlin Köpenick – medizinische Schwerpunkte und Herausforderungen“ (Knowledge gained from a 31-h power outage in Berlin Köpenick—medical problems and challenges) , 2021, Anaesthesist 7, Springer Medizin Verlag GmbH, Available online: https://doi.org/10.1007/s00101-021-00930-x , Last access: 2022-04-22

[BBR18] Marika Behnert, and Thomas Bruckner, “Causes and effects of historical transmission grid collapses and implications for the German power system”, Mar 2018, Contributions of the Institute for Infrastructure and Resources Management, ISSN 2364-4346, Available online: http://www.econstor.eu/escollectionhome/10419/107939, Last access: 2020-09-04

[BSB15] Bruce Schneier, “Secrets and Lies – Digital Security in a Networked World”, 2015, Wiley Computer Publishing, ISBN 0-471-25311-1

[BSC07] Bruce Schneier, “Real-ID: Costs and Benefits”, (2007-01-30), Schneier on Security Blog, Available online: https://www.schneier.com/blog/archives/2007/01/realid_costs_an.html, Last access: 2022-03-27

[BSN16] Bruce Schneier, “The Cost of Cyberattacks Is Less than You Might Think”, Sep 2016, Available online: https://www.schneier.com/blog/archives/2016/09/the_cost_of_cyb.html, Last access: 2022-04-30

[BSU16] Bruce Schneier, “The Unfalsifiability of Security Claims”, May 2016, Last access: 2022-04-30, available online: https://www.schneier.com/blog/archives/2016/05/the_unfalsifiab.html,

[CKS15] Michael A. Cusumano, Steven J. Kahl, and Fernando F. Suarez "Services, Industry evolution, and the competitive strategies of product firms", 2015, Strategic management journal 36 (4)

[DLA22] DLA Piper's cybersecurity and data protection team, "DLA Piper GDPR fines and data breach survey: January 2022", (Jan 2022), DLA.PIP.2031.22. Available online: https://www.all-about-security.de/wp-content/uploads/2022/01/Data-Breach-Report-2022.pdf, Last access: 2022-03-28

[ECB22] ECB / Eurostat, "Monthly number of working days (Monday to Friday) excluding public holidays (1990 - 2022 or 1995 - 2022)", 2022, Available online: https://ec.europa.eu/eurostat/cros/content/euro-area-and-eu-working-days-build-calendar-adjustment-regressor_en, Last access: 2022-04-27

[ECE17] European Commission, Eurostat, "NACE Rev. 2 : statistical classification of economic activities in the European Community", 2017, EU Publications Office, 2017, 978-92-79-04741-1, Available online: https://op.europa.eu/s/v4VP, Last access: 2022-02-24

[EDP22] European Data Protection Board (EDPB), "Polish SA: record fine imposed on Fortum Marketing and Sales Polska S.A. for personal data breach", 2022-03-17, Available online: https://edpb.europa.eu/news/national-news/2022/polish-sa-record-fine-imposed-fortum-marketing-and-sales-polska-sa-personal_en, Last access: 2022-04-15

[ENA22] Eurostat, "Main GDP aggregates per capita", dataset NAMA_10_PC, Apr 2022, available online: https://ec.europa.eu/eurostat/databrowser/view/NAMA_10_PC__custom_2590040/default/table?lang=en ,Last access: 2022-04-22

[ENF22] CMS Legal Services EEIG, "GDPR Enforcement Tracker", (2022-03-28) https://www.enforcementtracker.com/, Last access: 2022-03-28

[ENI16] ENISA (EU Cyber Security Agency), "Indispensable baseline security requirements for the procurement of secure ICT products and services", Dec 2016, Available online: https://www.enisa.europa.eu/publications/indispensable-baseline-security-requirements-for-the-procurement-of-secure-ict-products-and-services, Last access: 2022-03-30

[ESD19] EnergyShield, "Deliverable 8.1 Exploitation Plan Draft", non-public report, 2019-12-30

[ESD82] EnergyShield Deliverable 8.2 "Exploitation Report V1", Dec. 2020, (project internal document), European Union-H2020 Grant Agreement No. 832907, Work package 8 Exploitation

[EST21] Eurostat, "Household composition statistics", May 2021, available online: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=Household_composition_statistics , Last access: 2022-04-27

[EUE19] Directorate-General for Energy (European Commission) "EU energy in figures", Sep 2019, Available online: https://doi.org/10.2833/197947, Last access: 2022-02-15

[EUE21] Directorate-General for Energy (European Commission) “EU energy in figures“, Sep 2021, Available online: https://doi.org/10.2833/511498, Last access 2022-02-15

[FBA14] Sören Finster, and Ingmar Baumgart, “Privacy-aware Smart Metering: A Survey”, May 2014, IEEE Communications Surveys & Tutorials. 16(3), Available online: https://doi.org/10.1109/SURV.2014.052914.00090, Last access: 2022-04-01

[FOR21] Christopher Helman, “Cyber-Ransom Of $5m ‘Nothing’ To Colonial Pipeline, Which Has Paid Hundreds Of Millions In Dividends To Billionaire Koch Family”, Forbes, May 2021, Available online: https://www.forbes.com/sites/christopherhelman/2021/05/14/cyber-ransom-of-5m-nothing-to-colonial-pipeline-which-has-paid-hundreds-of-millions-in-dividends-to-billionaire-koch-family/?sh=5a721ccc2e6e, Last access: 2021-12-15

[HBR22] Tom Johansmeyer, “Market Needs More Money”, 2022-03-10, Harvard Business Review, Available online: https://hbr.org/2022/03/the-cyber-insurance-market-needs-more-money, Last access: 2022-04-25

[HCS22] Claudia Scholz, “Wann bei Cyberangriffen höhere Gewalt gilt“, Handelsblatt, 2022-02-14, Available Online: https://www.handelsblatt.com/politik/deutschland/lieferketten-wann-bei-cyberangriffen-hoehere-gewalt-gilt/28058656.html, Last access: 2022-04-12

[HEC20] Robert Heckman, "Managing the IT procurement process.", 2020, Enterprise Operations Management, Auerbach Publications. 367-383.

[HIQ21] “Does Home Insurance Cover Damage from a Power Outage?”, 2021, Available online: https://www.insurancequotes.com/home/home-insurance-power-outage, Last access: 2022-04-01

[HLA03] Maliha Haddad, and Anita La Salle, “Additional Costs And Risks In Software Acquisition Projects”, 2003, Journal of Business & Economics Research (JBER), Available online: https://doi.org/1.10.19030/jber.v1i8.3034

[IER19] Yasemin Irvin-Erickson, and Alexandra Ricks, “Identity theft and fraud victimization: What We Know about Identity Theft and Fraud Victims from Research- and Practice-Based Evidence”, Aug 2019, Center for Victim research report

[JRC19] European Commission, Joint Research Centre, T. Bouman, A. Longo, S. Giaccaria, T. Efthimiadis, “Societal appreciation of energy security. Volume 1, Value of lost load – households (EE, NL and PT)”, Jan 2019, Publications Office, https://doi.org/10.2760/139585

[KTG21] “Grid operator & PPC to compensate customers for power outages due to snow”, Feb 2021, Keeptalkinggreece.com, Available online: https://www.keeptalkinggreece.com/2021/02/20/greece-power-outages-snow-compensation/, Last access: 2022-04-01

[KTS09] Robert J Kauffman, and Juliana Y Tsai, “The Unified Procurement Strategy for Enterprise Software: A Test of the ‘Move to the Middle’ Hypothesis”, Journal of management Information Systems, 2009-09-01, Vol.26 (2), p.177-204, https://doi.org/10.2753/MIS0742-1222260208

[LBG18] A. Longo, T. Bouman, S. Giaccaria, and T. Efthimiadis, “Societal appreciation of energy security: Volume 1: Value of Lost Load - residential consumers (EE, NL and PT)”, 2018, EUR 29512 EN,

Publications Office of the European Union, Luxembourg, https://doi.org/10.2760/139585, JRC112728, Last access: 2022-04-01

[LGL94] R. Layard, and S. Glaister (Eds.). (1994, online version 2009). Cost-Benefit Analysis (2nd edition). Cambridge: Cambridge University Press. https://doi.org/10.1017/CBO9780511521942

[MDZ12] "Streit um Ersatz der Geräte" (Dispute over device replacements), 2012, Mitteldeutsche Zeitung, Available online: https://www.mz.de/lokal/dessau-rosslau/dessau-rosslau-streit-um-ersatz-der-gerate-2325971, Last access: 2022-02-15

[MEI21] Ministry of Energy State of Israel, "The Structure of the Energy Sector in Israel", Mar 2021, Available online: https://www.gov.il/BlobFolder/reports/israel_energy_sector/en/israel_energy_sector_en.pdf, Last access: 2022-02-09

[MZS21] Peter Mayer, Yixin Zou, and Florian Schaub, "Now I'm a bit angry: Individuals' Awareness, Perception, and Responses to Data Breaches that Affected Them", Aug 2021, Proceedings of the 30th USENIX Security Symposium, ISBN:9781939133243, Available online: https://www.usenix.org/conference/usenixsecurity21/presentation/mayer, Last access: 2022-04-15

[NAV18] „Verordnung über Allgemeine Bedingungen für den Netzanschluss und dessen Nutzung für die Elektrizitätsversorgung in Niederspannung (Niederspannungsanschlussverordnung - NAV) § 18 Haftung bei Störungen der Anschlussnutzung" (German low voltage grid code - §18 liability for outages), Available online: https://www.gesetze-im-internet.de/nav/__18.html, Last access: 2022-04-01

[OBS20] Nuno Vinha, (2020-04-13), "EDP alvo de ataque informático que bloqueou sistemas de atendimento aos clientes" (Engl. Translation: EDP targeted by computer attack that blocked customer service systems), Observador.pt, Available Online: https://observador.pt/2020/04/13/edp-alvo-de-ataque-informatico-que-bloqueou-sistemas-de-atendimento-aos-clientes/, Last access: 2022-04-25

[OP10] Alexander Osterwalder, and Yves Pigneur, "Business Model Generation: A Handbook for visionaries, game changers and challengers", Aug 2010, Wiley, ISBN:978-0470876411

[PEA16] J. Pearce, "Return on investment for open source scientific hardware development", Apr 2016, Science and public policy, Oxford University Press, 43 (2), pp.192-195, Available online: https://doi.org/10.1093/scipol/scv034, Last access: 2022-02-11

[PPP08] Patricia Pulliam Phillips, and Jack J. Phillips, "ROI Fundamentals - Why and When to Measure Return on Investment", 2008, Wiley

[PPP19] Patricia Pulliam Phillips, Jack J. Phillips, Gina Paone, and Cyndi Huff Gaudet, "Value for Money - How to Show the Value for Money for All Types of Projects and Programs in Governments, Nongovernmental Organizations", Nonprofits, and Businesses, 2019, John Wiley & Sons, Inc., ISBN 978-1-119-32265-8

[PRS07] J. Ploski, M. Rohr, P. Schwenkenberg, and W. Hasselbring, „Research issues in software fault categorization", Nov 2007, ACM SIGSOFT

Software Engineering Notes, 32(6), Available online: https://doi.org/10.1145/1317471.1317478, Last access: 2022-04-21

[SAF21] R. Silva, E. Alves, R. Ferreira, J. Villar; and C. Gouveia, "Characterization of TSO and DSO Grid System Services and TSO-DSO Basic Coordination Mechanisms in the Current Decarbonization Context." Energies 2021, 14, 4451. https://doi.org/10.3390/en14154451

[SOE11] SIGMA Joint initiative of the OECD and EU for Support for Improvement in Governance and Management, "Brief 16 – Public Procurement – Procurement by Utilities", Aug 2011, SIGMA Public Procurement Briefs, Available online: https://doi.org/10.1787/5js4vmnx5p28-en, Last access 2022-03-30

[SRO16] Sasha Romanosky, "Examining the costs and causes of cyber incidents", Dec 2016, Journal of cybersecurity, Volume 2, Issue 2, Available online: https://doi.org/10.1093/cybsec/tyw001, Last access: 2022-03-29

[SSR21] Sophos, "The State of Ransomware 2021", Apr 2021, Sophos Whitepaper, Available online: https://secure2.sophos.com/en-us/medialibrary/pdfs/whitepaper/sophos-state-of-ransomware-2021-wp.pdf, Last access: 2022-03-17

[SZE20] Sächsische Zeitung, "Das kostet ein Stromausfall im Stahlwerk", 2020-02-20, (German Newspaper Article)

[TAB10] Thomas Petermann, Harald Bradke, Arne Lüllmann, Maik Poetzsch, and Ulrich Riehm, Büro für Technikfolgen-Abschätzung beim Deutschen Bundestag (TAB), "TA-Projekt: Gefährdung und Verletzbarkeit moderner Gesellschaften – am Beispiel eines großräumigen und langandauernden Ausfalls der Stromversorgung" Nov 2010, ISSN: 2364-2599, Available online: https://doi.org/10.5445/IR/1000103291 Last-Access: 15.02.2022

[UNa08] United Nations, Department of Economic and Social Affairs, "International Standard Industrial Classification of All Economic Activities", 2008, Rev. 4, ST/ESA/STAT/SER.M/4/Rev.4, Available online: https://www.bundesbank.de/resource/blob/612626/5cc47990a81e09543f71928692ad9568/mL/isic-rev-4-data.pdf

[UPN20] UK Power Networks, "Electricity guaranteed standards relating to power cuts", 2020, Available online: https://www.ukpowernetworks.co.uk/-/media/files/customer-care/electrical-guaranteed-standards.ashx, Last access: 2022-04-22

[WIR16] Kim Zetter, (2016-03-03), "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid", wired.com, Available Online: https://www.wired.com/2016/03/inside-cunning-unprecedented-hack-ukraines-power-grid/, Last access: 2022-04-26

[WTW20] Glyn Thoms, "Cyber claims analysis report", Jul 2020, Willis Towers Watson analysis report, Available online: https://www.wtwco.com/en-NZ/Insights/2020/07/cyber-claims-analysis-report, Last access: 2022-04-26

7. APPENDIX A - QUESTIONNAIRES

In the following, the questionnaires provided to the project partners are presented. The single results / answers are not included in the report, because the answers could include confidential business information, such as pricing strategy. The primary purpose of the answers is to get data for calibrating the business model.

For the business case analysis, the different pricing / license models are unified and simplified – this means that the questions regarding the price ranges implicitly suggest a certain license policy (e.g., upfront initial license instead of subscription model) that might not match with the actual license and pricing model of the tool provider. However, this is not a too big issue because for instance, subscription models can be translated to financially similar initial-license-fee models and open sources components can have a license fee of zero.

We decided to split up the end-user questionnaire into two versions (presented in Sections 0 and 7.3), to address that the two GENCOs in the project are magnitudes smaller (regarding employees and revenue) than the three grid operators. Since we determined in a previous analysis that the primary target customers are larger energy companies, the rollout scenario in the business model chapter conforms to the one used in Section 0 and a scaled down scenario is used for the small/medium energy companies in the questionnaire in Section 7.3.

7.1. TECHNOLOGY PROVIDER QUESTIONNAIRE

This survey is part of WP8 (Exploitation) Task 8.2 Business Cases. It is not about a field trial scenario – it is about a reasonable rollout and the business case of the EnergyShield toolkit provided by a general contractor to the customer for projects of 2-5 tools. We need reasonable cost and price estimates for your tool to make our numbers more in the model realistic.

We assume a “roll-out” scenario, so it is a larger installation than in the field test and it is running in production. We assumptions a medium-sized distribution grid operator (DSO):

- 1,5 million private household contracts for electrical energy, yearly turnover of €1 billion per year
- 1.500 employees: As rollout for the SBA, we assume that the majority employees are covered (at least those with access to network/IT).
- 100 high-voltage/low-voltage substations, and 10.000 medium-voltage/low-voltage substations. The rollout for Anomaly Detection is assumed for 6 MV/HV substations with each approx. 5-20 measurements. Even in the case of the complete failure/manipulation of the central SCADA, operators could get a reasonable feeling based on these measurements

- 3 APIs need to be protected by DDoSM: e.g., for smart metering (AMI), communication with smaller renewables, data exchange with the regulator
- For the VA, we assume to cover most critical points of the IT- and OT-Network (6 high value assets). Models of network and system-architecture are modeled in the VA tool, vulnerability scans are executed in three network zones, and configuration files from three sources such as firewalls are imported. Five workshop iterations with the customers IT and security teams for both the IT- and OT-network are used to identify and simulate the system model.
- An (initial) rollout of the SIEM would cover 30 major IT- and OT-systems/applications of the more than 100+ central applications a typical DSO might have. For simplicity PCs or Laptops are not included into the estimation. For each application, there is at least an integration of log-files (e.g., login failures) and instrumentation with probes (e.g., health checks). The SIEM will have customized dashboards and correlations that integrate the single information into a complete picture.

All costs should be full costs, which also covers its share on company overhead, such as office rent etc. The product development and platform operation costs are not in the project costs - they would be covered by license/platform costs.

Question 1

Project costs until it is running in production (only your tool costs in the toolkit project but with toolkit integration costs included). It should include all preparations, execution of workshops, trainings, etc. (we assume installation in an EnergyShield-on-prem-environment in the DSO's data center). We use here the 3-point-PERT-estimation method:

- (1.1) Optimistic cost estimate (€):
  - Your answer:
- (1.2) Pessimistic cost estimate (€)
  - Your answer:
- (1.3) Realistic cost estimate (€)
  - Your answer:

Question 2

Project Price - which "project list price" would you start the negotiation with (for only this part of the toolkit…) in this market:

- Price in year 1
  - (2.1) Realistic estimate:
    - Your answer:
  - (2.2) Typical negotiation spread (standard deviation):
    - Your answer:

Question 3

Yearly service & maintenance and yearly license/platform fee (including additional consulting if this is typical). It should also cover server costs in the cloud if additionally needed (e.g., for DDoSM protection). For the SIEM it is especially about security updates, 2nd level support, and a limited contingent of consulting (less than 10 days).

- (3.1) Yearly license/platform price in year 1,2,3,4, …
  - Your answer:
- (3.2) Yearly service and maintenance fee (independently if used or not) price:
  - Your answer:
- Yearly costs that have to be covered (license/platform/service/maintenance) by the contract. It does not need to cover costs that are part of the general Energy Shield infrastructure.
  - (3.3) Optimistic cost estimate (€):
    - Your answer:
  - (3.4) Pessimistic cost estimate (€):
    - Your answer:
  - (3.5) Realistic cost estimate (€):
    - Your answer:

Question 4 - Benefits from being part of the EnergyShield toolkit and its toolkit sales process

- (4.1) Benefit from the platform or from the EnergyShield toolkit provided as a bundle to the customer together with an integrator / general contractor:
    - Your answer:
  - How much of that benefit would result from a preinstalled EnergyShield platform reduce your costs or increase your business values?
    - Your answer:
- (4.2) Can you give a feeling what you thing regarding the security benefit of the SBA's integration within the toolkit in % compared to an unintegrated SBA?
  - Your answer:

7.2. LARGE ENERGY COMPANY QUESTIONNAIRE

This survey is part of WP8 (Exploitation) Task 8.2 Business Cases. The goal is to identify quantitative and financial arguments for other potential customers to select the EnergyShield toolkit. It is not about a field trial scenario - it is about a reasonable rollout. All answers are confidential and will only anonymized or generalized be part of the public report. Please provide rough estimates and spontaneous best guesses from your point of view for a company like yours.

7.2.1. POTENTIAL COSTS RELATED TO THE ENERGY-SHIELD TOOLKIT

What is your opinion about a **reasonable price** range for an initial project price and yearly service contract price **for a company like yours** for the toolkit with all five tools? The price range should be a fair compromise between vendor and buyer.

- 1,5 million private household contracts for electrical energy, yearly turnover of €1 billion per year
- 1.000 employees: As rollout for the SBA, we assume that the majority employees are covered (at least those with access to network/IT).
- 100 high-voltage/low-voltage substations, and 10.000 medium-voltage/low-voltage substations. The rollout for Anomaly Detection is assumed for 6 MV/HV substations with each approx. 5-20 measurements. Even in the case of the complete failure/manipulation of the central SCADA, operators could get a reasonable feeling based on these measurements
- 3 APIs need to be protected by DDoSM: e.g., for smart metering (AMI), communication with smaller renewables, data exchange with the regulator
- For the VA, we assume to cover most critical points of the IT- and OT-Network (6 high value assets). Models of network and system-architecture are modelled in the VA tool, vulnerability scans are executed in three network zones, and configuration files from three sources such as firewalls are imported. Five workshop iterations with the customers IT and security teams for both the IT- and OT-network are used to identify and simulate the system model.
- An (initial) rollout of the SIEM would cover 30 major IT- and OT-systems/applications of the more than 100+ central applications a typical DSO might have. For simplicity PCs or Laptops are not included into the estimation. For each application, there is at least an integration of log-files (e.g., login failures) and instrumentation with probes (e.g., health checks). The SIEM will have customized dashboards and correlations that integrate the single information into a complete picture.
- The EnergyShield platform is installed in your data centre with remote access.

7.2.1.1. INITIAL PROJECT PRICE INCLUDING THE LICENSES

Initial project price with local hardware included (AD-probes), consulting included, installation of toolkit, licenses, etc.

Your answer for a reasonable price for the scenario described above:

- XXX.XXX € VU
- XXX.XXX € SBA
- XXX.XXX € AD,
- XXX.XXX € DDOS,
- XXX.XXX € SIEM +
- XXX.XXX € toolkit platform setup (Server hardware provided by customer)
- Total = XXX.XXX

Do you have additional remarks on the price range a company like yours would accept?

7.2.1.2. YEARLY SERVICE CONTRACT

What is your opinion of a reasonable yearly service contract that EnergyShield could ask for from a company like yours?

Your answer:

- XXX.XXX € VU (2 update/review/what-if-analysis workshops + license)
- XXX.XXX € SBA (repeated executions, or with to other employees)
- XXX.XXX € AD (patches and 2nd level support, license for tool)
- XXX.XXX € DDOS (protection platform in front of the APIs, and 2nd level support)
- XXX.XXX € SIEM (contingent for extensions, 2nd level support contingent)
- XXX.XXX EnergyShield toolkit (patch management, updates, 1st level support)
- = XXX.XXX € / year
-

7.2.2. SYNERGY BENEFITS – LESS EFFORT WITH A TOOLKIT

The purchasement, the specification and installation, etc. of software can have significant effort for an energy sector company. For ERP system, the internal effort-costs might even be much higher than the product and project price payed to the vendor/integrator.

How large do you estimate the benefit from having one toolkit with **5 pre-integrated** tools provided, coordinated, and operated by a single general contractor in contrast to having 3-5 independent smaller projects? Our numbers are our first guess for a small/medium GENCO like you company – they might be completely wrong – what do you think?

7.2.2.1. SYNERGIES IN SPECIFICATION AND INSTALLATION PHASE

IT- and security departments usually need to be involved in the definition how security tools operate in the companies' environment, and have to participate in defining for instance, network connections, firewall settings, VPN configuration, remote access maintenance, and allowed frameworks / operating systems / data bases.

Your answer:

- 5 tools independently: XX - XX person days effort for your company
- 5 tools as part of the EnergyShield toolkit: XX - XX person days effort for your company

⇨ XX% potential synergies (i.e., less own effort)

7.2.2.2. SYNERGIES IN PURCHASEMENT

Are there similar benefits in the selection and purchasement process? The Energy Shield toolkit would provide a single contract, a single sales contract, a single decision process.

Your answer:

- 5 tools independently: XX – XX person days effort for your company
- 5 tools as part of EnergyShield the toolkit: XX-XX person days effort for your company

⇨ XX% - XX% reduction during purchasement

7.2.2.3. SYNERGIES IN OPERATION

In operation, it is easier to have for 5 integrated tools with a single service provider that provides 1st level support (and some basic 2nd level support), and security patches, instead of heaving 5 different contractors. Additionally, only one remote access has to be monitored and maintained from your side.

Your answer:

- 5 tools independently: XX-XX person days / year effort for your company
- 5 tools as part of the EnergyShield toolkit: XX-XX person days / year customer effort

⇨ XX%-XX% effort reduction

7.2.3. POTENTIAL BENEFITS FROM CYBERSECURITY PROTECTION

7.2.3.1. DIRECT LEGAL REQUIREMENTS / FINES

Is there a direct legal requirement to have at least one of the tools of the toolkit for companies such as your company in your national regulation? What happens, if such a requirements are not met?

7.2.3.2. LIABILITIES FOR OUTAGES

A successful attack against a control system could cause temporary power outages. Would there be any (especially financial) liabilities for compensating grid customers for such a power outage in your national regulation or fines from the regulator?

7.2.3.3. GDPR

Is there a significant financial risk that a company like your company would have to deal with high fines if customer data is stolen from your business systems / ERP-systems?

7.2.3.4. CYBERSECURITY INSURANCE

Is it typical for a company like your company to have a cybersecurity insurance? Does the insurance require particular technologies, such as those in the Energy Shield toolkit?

7.3. MEDIUM / SMALL ENERGY COMPANY QUESTIONNAIRE

This survey is part of WP8 (Exploitation) Task 8.2 Business Cases. The goal is to identify quantitative and financial arguments for other potential customers to select the EnergyShield toolkit. It is not about a field trial scenario - it is about a reasonable rollout. All answers are confidential and will only anonymized or generalized be part of the public report. Please provide rough estimates and spontaneous best guesses from your point of view for a company like yours.

7.3.1. POTENTIAL COSTS RELATED TO THE ENERGY-SHIELD TOOLKIT

What is your opinion about a **reasonable price** range for an initial project price and yearly service contract price **for a company like yours** for the toolkit with all five tools? The price range should be a fair compromise between vendor and buyer.

- Approximately 10-20 most relevant measurement points for anomaly detection.
- Two external APIs would be protected by DDoSM (e.g., data exchange with grid operator and market).
- All employees with network access will participate in two initial iterations of SBA with yearly refresh.
- Vulnerability Analysis and threat simulation with 1,5 workshops. Vulnerability scans will be executed.
- The SIEM will have probes on all critical systems in IT and OT network. It will additionally integrate the data from the other EnergyShield tools.
- The EnergyShield platform is partly installed in a secure cloud environment with some components in a single VM in your environment.

7.3.1.1. INITIAL PROJECT PRICE INCLUDING THE LICENSES

Initial project price with local hardware included (AD-probes), consulting included, installation of toolkit, licenses, etc.

Your answer for a reasonable price for the scenario described above:

- XXX.XXX € VU
- XXX.XXX € SBA
- XXX.XXX € AD,
- XXX.XXX € DDOS,
- XXX.XXX € SIEM +
- XXX.XXX € toolkit platform setup (Server hardware provided by customer)
- Total = XXX.XXX

Do you have additional remarks on the price range a company like yours would accept?

7.3.1.2. YEARLY SERVICE CONTRACT

What is your opinion of a reasonable yearly service contract that EnergyShield could ask for from a company like yours?

Your answer:

- XX€ VU (possibility to make changes to the model and simulate it – no consulting included; only technical support for errors and security updates)
- XX € SBA (repeated execution, or with new employees)
- XX € AD (patches and 2nd level support, license for tool and platform)
- XX € DDOS (protection platform in front of the APIs, and 2nd level support)
- XX € SIEM (2nd level support and single of days consulting contingent)
- XX € EnergyShield toolkit and general contractor services (patch management, updates, limited 1st level support – only office hours)
- = XX € / year
-

7.3.2. SYNERGY BENEFITS – LESS EFFORT WITH A TOOLKIT

The purchasement, the specification and installation, etc. of software can have significant effort for an energy sector company. For ERP system, the internal effort-costs might even be much higher than the product and project price payed to the vendor/integrator.

How large do you estimate the benefit from having one toolkit with **5 pre-integrated** tools provided, coordinated, and operated by a single general contractor in contrast to having 3-5 independent smaller projects? Our numbers are our first guess for a small/medium GENCO like you company – they might be completely wrong – what do you think?

Your answer:

- XX-XX days effort on your side for evaluation, purchasement, installation of a 5 **toolkit** package from a single general contractor
- XX-XX days effort on your side for evaluation, purchasement, installation of a 5 tools independently that are **not part of a toolkit**, including the effort to evaluate upfront whether the tools are interpretational. Contracts with 5 different vendors.

7.3.3. POTENTIAL BENEFITS FROM CYBERSECURITY PROTECTION

7.3.3.1. COVERAGE FOR FINANCIAL LOSS & CYBERSECURITY INSURANCE

Is it typical for a company like your company to have a cybersecurity insurance that covers financial loss due to service interruption from a cyber-attack? Do you know whether such insurances required particular technologies, such as those in the Energy Shield toolkit?

7.3.3.2. DIRECT LEGAL REQUIREMENTS / FINES

Is there a direct legal requirement to have at least one of the tools of the toolkit for companies such as your company in your national regulation? What happens, if such a requirements are not met?

7.3.3.3. LIABILITIES FOR OUTAGES

A successful attack against your control system could cause temporary shutdown. Would there be any (especially financial) liabilities for customers?

7.3.3.4. GDPR

Do you consider a company as your company having a significant financial risk if customer data is stolen from your business systems / ERP-systems from the GDPR?

8. APPENDIX B – SOCIO-ECONOMIC DATA

In the following, original data from Eurostat, DG Energy, and the Structural Business Statistics Survey (SBS) are shown. The Eurostat data can be browsed online (https://ec.europa.eu/eurostat/databrowser). The other data is this chapter is from [EUE21].

The sources categorize data into NACE Rev. 2 categories, which can are the categorizations used by the EU. The two NACE Rev. 2 [ECE17] categories D35 ("Electricity, Gas, Steam and Air Conditioning Supply") and D35.1 ("Electric power generation, transmission and distribution") seem to be identical to the corresponding United Nations ISIC Rev. 4 categories [UNa08]. Segment D35.1 includes energy production, transmission, distribution, and trading including activities of retailers/suppliers. D35 and D35.1 do not include without water and sewage utilities and without long distance gas pipelines ([ECE17], p. 202).

8.1. NUMBER OF EMPLOYEES

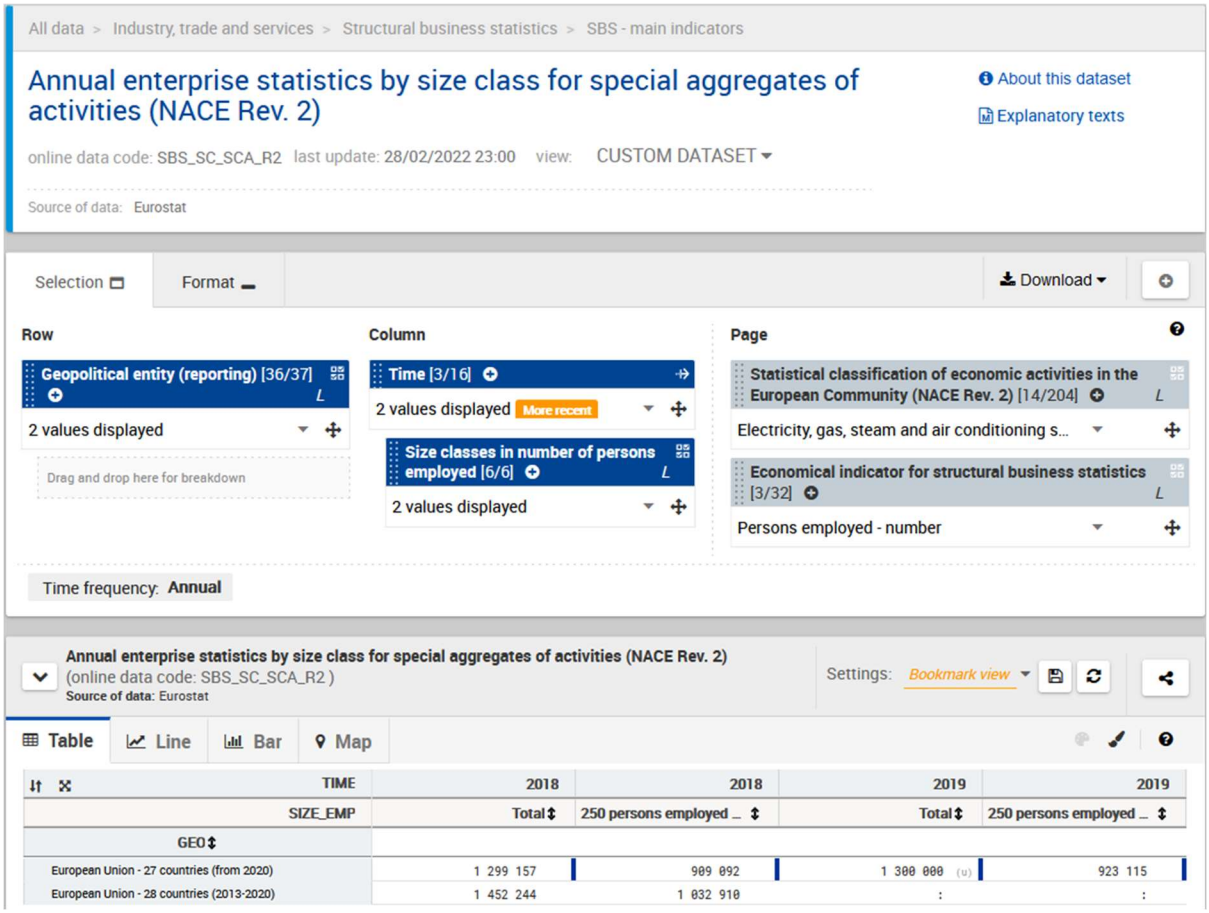

Figure 6: Number of employees for companies in segment D35 from the Eurostat SBS_SC-SCA-R2 dataset.

As shown in Figure 6, a large share of the employees in the European energy sector are working in large companies with 250 or more employees. Figure 7 shows that a majority of EU energy sector employees work in the area of electrical power. A bookmark on the data set shown in Figure 6 is stored here: https://ec.europa.eu/eurostat/databrowser/bookmark/8821d8fc-8077-4110-93c0-24f5803c10e9?lang=en

3.2.3 Number of Persons Declared as Employed in the Energy Sector

ENTERPRISES SURVEY – EU27_2020

	2019
D35: Electricity, Gas, Steam and Air Conditioning Supply	*1379747*
D35.1: Electricity Power Generation, Transmission and Distribution	*1045051*
35.11: Production of Electricity	*450296*
35.12: Transmission of Electricity	*40463*
35.13: Distribution of Electricity	*198552*
35.14: Trade of Electricity	*110944*
D35.2: Manufacture of Gas; Distribution of Gaseous Fuels through Mains	*96044*
35.21: Manufacture of Gas	*11526*
35.22: Distribution of Gaseous Fuels through Mains	*34894*
35.23: Trade of Gas through Mains	*29414*
D35.3: Steam and Air Conditioning Supply	*108382*
35.30: Steam and Air Conditioning Supply	*114062*

Italics, blue: DG Energy Estimates.

Source: Eurostat, Structural Business Statistics Survey (SBS), May 2021

Figure 7: Compressed illustration energy sector employees ([EUE21], page 149).

8.2. TURNOVER

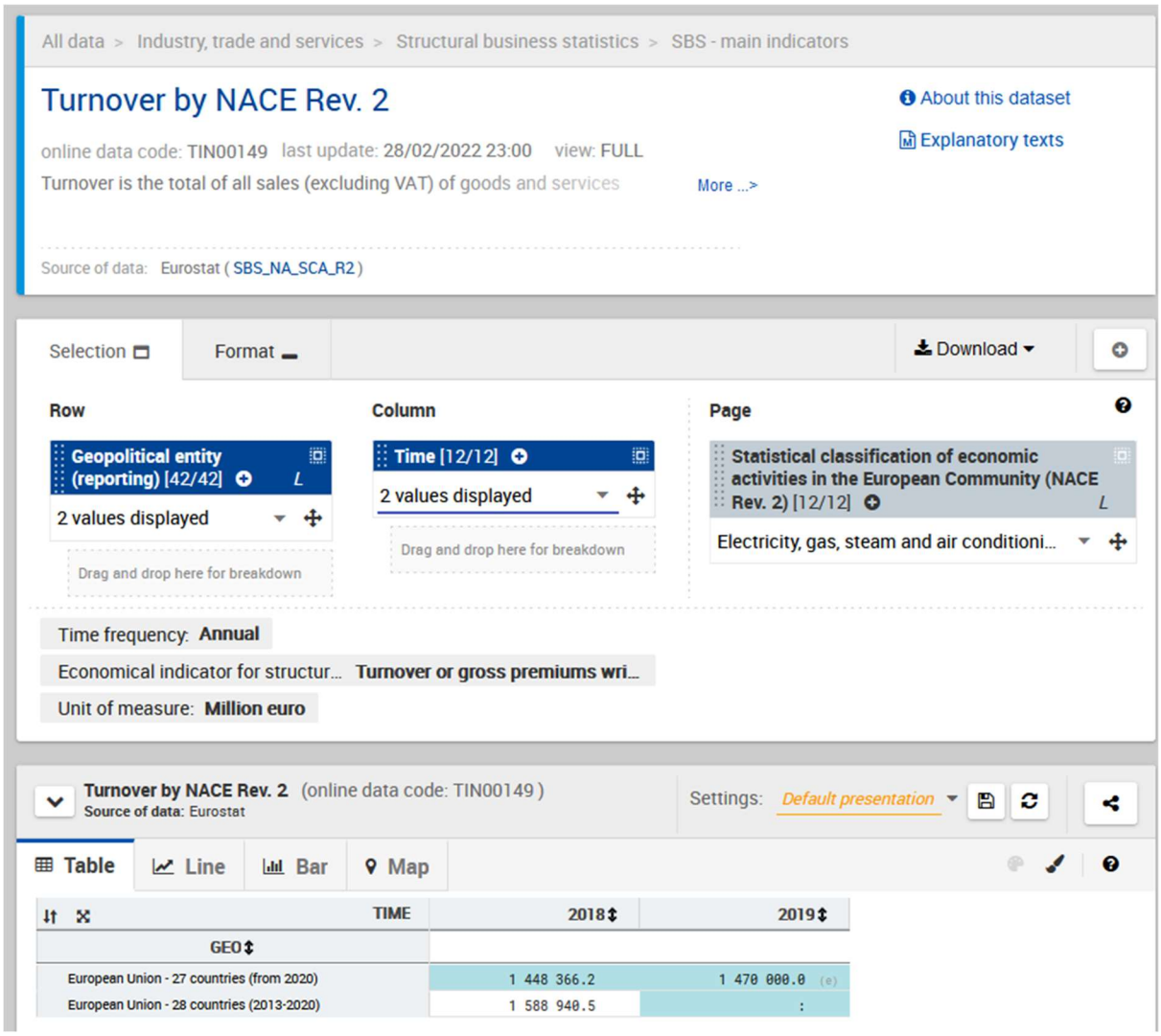

Figure 8: Turnover in million € for segment D35 of Eurostat's SBS_NA-SCA-R2 dataset.

A bookmark on the data presented in Figure 8 is stored here: https://ec.europa.eu/eurostat/databrowser/bookmark/31b243c7-60d8-435d-a4b5-781d3d9811b4?lang=en.

3.2.2 Turnover in the Energy Sector

ENTERPRISES SURVEY – EU27_2020

Mio EUR	2019
D35: Electricity, Gas, Steam and Air Conditioning Supply	*1 456 779*
D35.1: Electricity Power Generation, Transmission and Distribution	*1 165 231*
35.11: Production of Electricity	*224 559*
35.12: Transmission of Electricity	*55 942*
35.13: Distribution of Electricity	*122 833*
35.14: Trade of Electricity	*412 272*
D35.2: Manufacture of Gas; Distribution of Gaseous Fuels through Mains	*218 575*
35.21: Manufacture of Gas	*24 392*
35.22: Distribution of Gaseous Fuels through Mains	*21 917*
35.23: Trade of Gas through Mains	*129 447*
D35.3: Steam and Air Conditioning Supply	*34 367*
35.30: Steam and Air Conditioning Supply	*27 409*

Italics, blue: DG Energy Estimates.

Source: Eurostat, Structural Business Statistics Survey (SBS), May 2021

Figure 9: Compressed turnover breakdown for D35 based on [EUE21], page 145.

Figure 9 shows that most of D35's turnover is in D35.1, which is the focus of our analysis

8.3. NUMBER OF COMPANIES

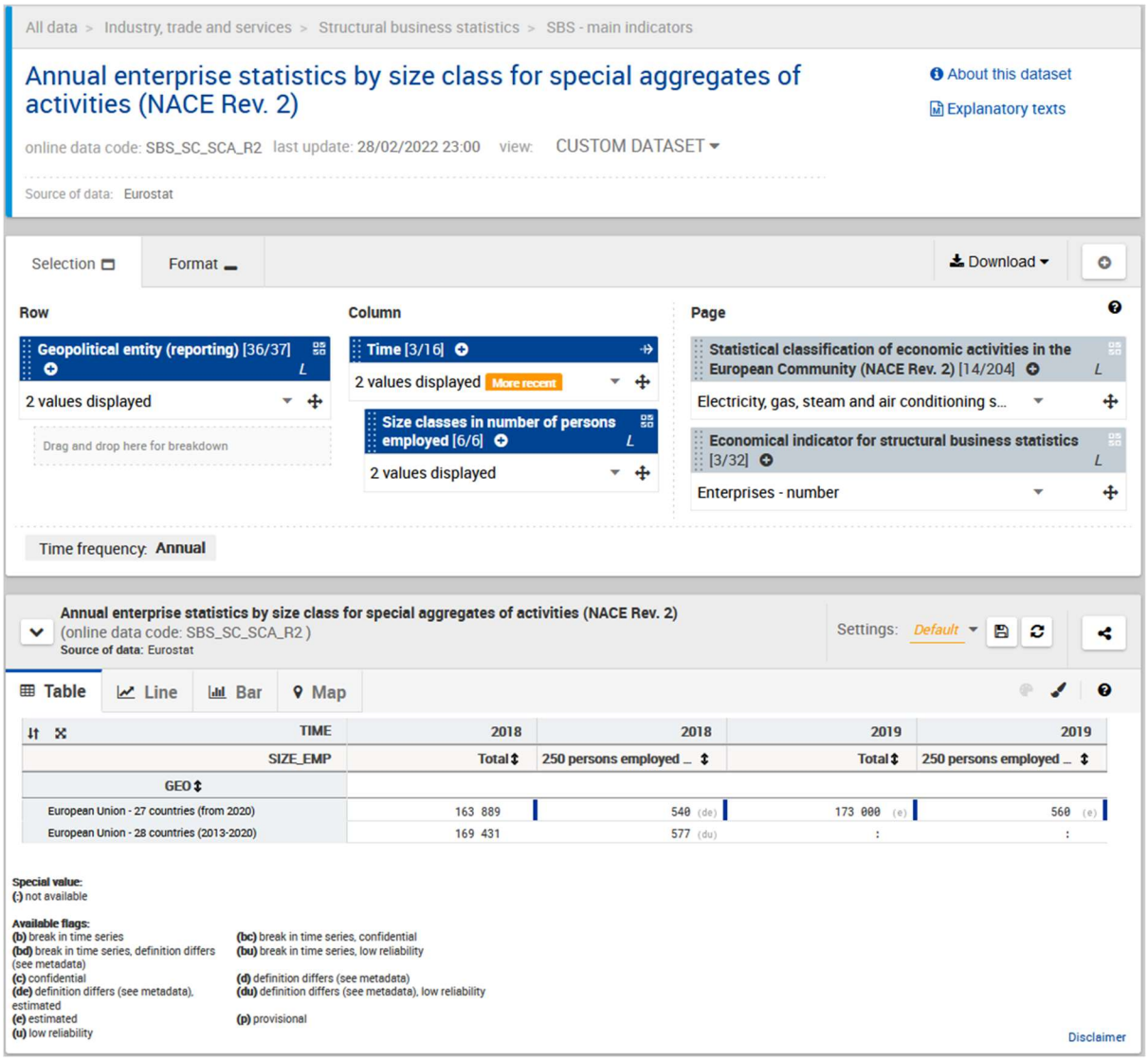

Figure 10: Number of companies with more than 250 employees in segment D35 from the Eurostat SBS_SC_SCA_R2 dataset.

As shown in Figure 10, not many of the 173.000 companies in the D35 energy segment are larger than 250 employees – our current focus is on large companies with more than 250 employees. A bookmark on the data selected in Figure 10 is stored here: https://ec.europa.eu/eurostat/databrowser/bookmark/5c465049-1b5b-44da-a668-68f9bb51255f?lang=en.

3.2.1 Number of Enterprises in the Energy Sector

ENTERPRISES SURVEY – EU27_2020

		2019
D35:	Electricity, Gas, Steam and Air Conditioning Supply	*162 989*
D35.1:	Electricity Power Generation, Transmission and Distribution	*151 605*
	35.11: Production of Electricity	*133 975*
	35.12: Transmission of Electricity	*600*
	35.13: Distribution of Electricity	*2 521*
	35.14: Trade of Electricity	*4 240*
D35.2:	Manufacture of Gas; Distribution of Gaseous Fuels through Mains	*5 238*
	35.21: Manufacture of Gas	*3 823*
	35.22: Distribution of Gaseous Fuels through Mains	*594*
	35.23: Trade of Gas through Mains	*691*
D35.3:	Steam and Air Conditioning Supply	*6 160*
	35.30: Steam & Air Conditioning Supply	*6 160*

Italics, blue: DG Energy Estimates.

Source: Eurostat, Structural Business Statistics Survey (SBS), May 2021

Figure 11: Compressed breakdown of enterprises in D35 based on [EUE21], page 141.

9. APPENDIX C – ROI-TABLE

Year	Total cum. costs	Cum. ROI-Abs R1	ROIR 1	Cum.-ROI-Abs R2	ROI R2	R3=R2+Public	ROI R3	Total cum. costs	Cum. ROI-Abs R1	ROI R1	Cum. ROI-Abs R2	ROI R2	R3=R2+Public	ROI R3
	DSO1							DSO2						
1	994.636€	470.800€	-53%	294.841€	-70%	2.752.219€	177%	1.271.836€	811.557€	-36%	510.045€	-60%	8.395.724€	560%
2	1.412.456€	941.601€	-33%	589.682€	-58%	5.504.438€	290%	1.843.083€	1.623.113€	-12%	1.020.090€	-45%	16.791.447€	811%
3	1.830.276€	1.412.401€	-23%	884.523€	-52%	8.256.658€	351%	2.414.330€	2.434.670€	1%	1.530.135€	-37%	25.187.17 €	943%
4	2.248.096€	1.883.201€	-16%	1.179.363€	-48%	11.008.877€	390%	2.985.577€	3.246.227€	9%	2.040.180€	-32%	33.582.895€	1025 %
5	2.665.916€	2.354.002€	-12%	1.474.204€	-45%	13.761.096€	416%	3.556.823€	4.057.783€	14%	2.550.225€	-28%	41.978.618€	1080 %
6	3.083.737€	2.824.802€	-8%	1.769.045€	-43%	16.513.315€	435%	4.128.070€	4.869.340€	18%	3.060.271€	-26%	50.374.342€	1120 %
7	3.501.557€	3.295.602€	-6%	2.063.886€	-41%	19.265.534€	450%	4.699.317€	5.680.897€	21%	3.570.316€	-24%	58.770.065€	1151 %
8	3.919.377€	3.766.403€	-4%	2.358.727€	-40%	22.017.754€	462%	5.270.564€	6.492.453€	23%	4.080.361€	-23%	67.165.789€	1174 %

Table 17: ROI calculation results.

Developing the cyber-toolkit that protects your energy grid

www.energy-shield.eu