



# ENERGY SHIELD

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

INNOVATION ACTION

H2020 Grant Agreement Number: 832907

### WP9 MANAGEMENT

## D9.1 SOCIETAL IMPACT REPORT

#### Document info

Contractual delivery	30/06/2022
Actual delivery	30/06/2022
Responsible Beneficiary	SIMAVI
Contributing beneficiaries	All
Version	1.0



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



**DOCUMENT INFO**

<b>Document ID:</b>	<b>D9.1</b>
<b>Version date:</b>	30/06/2022
<b>Total number of pages:</b>	49
<b>Abstract:</b>	This task aims at monitoring and evaluating societal impact of the project
<b>Keywords</b>	Standardisation, policy, societal impact

**AUTHORS**

<b>Name</b>	<b>Organisation</b>	<b>Role</b>
<b>Otilia Bularca</b>	SIMAVI	Overall Editor/
<b>Lavinia Dinca</b>	SIMAVI	Contributor
<b>Ana-Maria Dumitrescu</b>	SIMAVI	Section editor

**REVIEWERS**

<b>Name</b>	<b>Organisation</b>	<b>Role</b>
<b>Matthias Rohr</b>	PSI	Overall Reviewer
<b>Roysten Dsouza</b>	FOR	QA Reviewer

**VERSION HISTORY**

<b>V0.1</b>	10/04/2022	Table of contents
<b>V0.2</b>	12/05/2022	Release of 2nd draft
<b>V0.3</b>	12/06/2022	Feedback & contributions from partners
<b>V0.4</b>	20/06/2022	Version ready for internal review
<b>v1.0</b>	30/06/2022	Final version, released to the EC

## EXECUTIVE SUMMARY

This deliverable presents the societal impact that the EnergyShield project managed to accomplish up until the date of the delivery of this report. This document details how the tools as individual components and the EnergyShield toolkit as a whole can help society by securing one of the most relied upon critical infrastructures: the energy grid.

The impact of the R&I investments and, consequently the scientific advancements and the deployment of new concepts and technologies is positive for the society in general. However, the technological development and the social needs need to be matched to manage to significantly influence the development of individuals, groups of people and the society in general.

Energy literacy principles correlate the social expectations with the technology advancement and with the impacts that those may have.

On the other hand, most cyber-attacks have a human and social component and as such, may also have behavioural impact.

An overview of risks and impacts raised by the objectives and the core concept of the technology being developed in the EnergyShield project is provided within this report.

## TABLE OF CONTENTS

EXECUTIVE SUMMARY .....	3
Table of Contents .....	4
List of figures .....	5
List of tables .....	6
Acronyms .....	7
1. Introduction .....	8
1.1. Scope and objectives .....	8
1.2. Structure of the report .....	8
1.3. Task dependencies .....	8
2. Societal Challenges & Principles .....	9
2.1. Research and innovation challenges .....	11
2.2. Energy literacy principles .....	12
2.3. Societal “face” of cyber-attacks .....	13
2.4. Proposed approach .....	17
3. Societal impact of EnergyShield tools .....	20
3.1. Societal Impact Assessment (SIA) of tools .....	20
3.1.1. SIA of VA tool .....	20
3.1.2. SIA of SBA tool .....	23
3.1.3. SIA of AD tool .....	27
3.1.4. SIA of DDoSM tool .....	31
3.1.5. SIA of SIEM tool .....	34
3.1.6. SIA of EnergyShield toolkit .....	38
3.2. Cross -evaluation of tools .....	42
4. Conclusion .....	45
5. References .....	46

## LIST OF FIGURES

Figure 1. Semantic fusion and classification.....	10
Figure 2. Focus of societal challenges and impact of R &I investments .....	11
Figure 3. The key concepts of energy literacy [CLE22] .....	12
Figure 4. Societal impact of using technologies and methods.....	13

## LIST OF TABLES

Table 1. Survey to identify the social impact of EnergyShield .....	18
Table 2. Societal impact assessment of VA tool in the EnergyShield project.....	20
Table 3. Societal impact assessment of SBA tool in the EnergyShield project .....	23
Table 4. Societal impact assessment of AD tool in the EnergyShield project .....	27
Table 5. Societal impact assessment of DDoSM tool in the EnergyShield project ..	31
Table 6. Societal impact assessment of SIEM tool in the EnergyShield project.....	34
Table 7. Societal impact assessment of EnergyShield toolkit in the EnergyShield project .....	39
Table 8. Societal impact factors analysis.....	42

## ACRONYMS

ACRONYM	DESCRIPTION
AD	Anomaly Detection
DDoSM	Distributed Denial of Service Mitigation
ELS	Ethical, legal and societal aspects
EPES	Electrical Power and Energy System
PIA	Privacy impact assessment
PII	Personal Identifiable Information
SBA	Security Behaviour Analysis
SDLC	Secure Development Life Cycle
SGAM	Smart energy Grid Architecture Model
SIA	Societal Impact Assessment
SIEM	Security Information and Event Management
VA	Vulnerability Assessment

## 1. INTRODUCTION

### 1.1. SCOPE AND OBJECTIVES

This deliverable presents the societal impact that the EnergyShield project has at the end of the project. This document details how the tools can help society by security one of the most relied on critical infrastructures: the energy grid.

### 1.2. STRUCTURE OF THE REPORT

The present document is structured in two parts aiming at providing

- 1) an overview of the societal challenges, principles, and drivers,
- 2) an assessment of the Energy Shield tools alongside with some recommendations to reduce the potential negative impact of cyberattacks on the individuals as part of the society and increase secure use and trust in technological advancement.

These parts are prefaced by an introduction and the document ends with some brief conclusions and the relevant references.

### 1.3. TASK DEPENDENCIES

While this report focuses on the societal impact assessment, the related ethical and legal aspects are approached in D1.6 [ESH16].

## 2. SOCIETAL CHALLENGES & PRINCIPLES

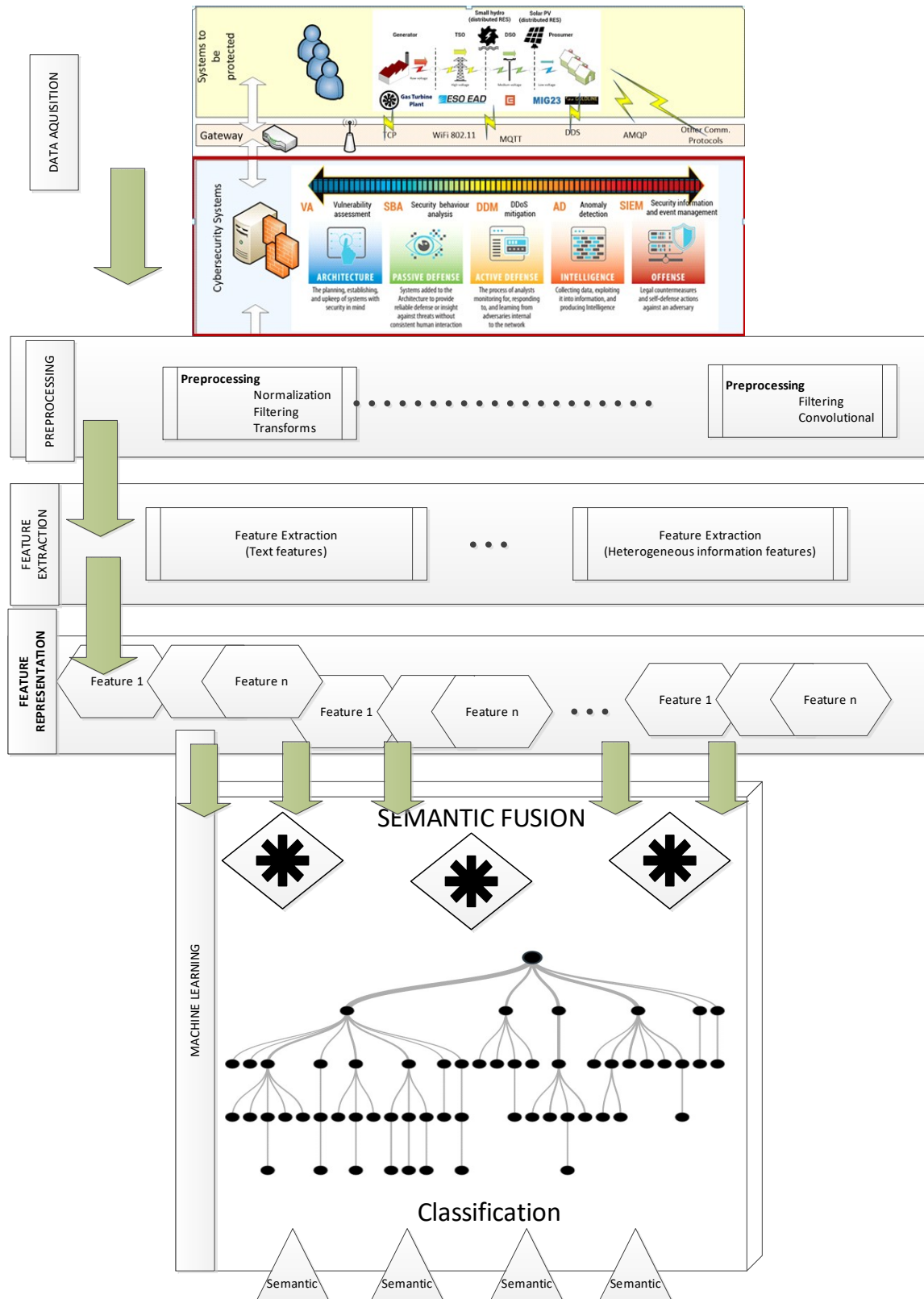
EnergyShield (Integrated Cybersecurity Solution for the Vulnerability Assessment, Monitoring and Protection of Critical Energy Infrastructures) is an innovation action that brings together cybersecurity and energy infrastructure protection, while involving stakeholders from the entire EPES value chain.

The scope of the EnergyShield project is situated at the intersection of information technology and energy sector advancing a toolkit to defend electrical power and energy system actors against cyber security attacks.

The integrated view of the proposed EnergyShield architecture is based on two architectural perspectives, 4+x [KRU95] and SGAM [CEN12], iconic for their respective fields: IT and the energy sector, mainly the electric energy grid. Mapping a canonical model with a reference model created a novel and unique architectural design that accommodates the needs and technological advancements proposed by EnergyShield partners.

This architecture of the EnergyShield system is based on a knowledge components that address the interconnection and integration of the separate tools: Vulnerability Assessment (VA), Anomaly Detection (AD), Security Behaviour Analysis (SBA), Distributed Denial of Service Mitigation (DDoSM) and Security information and Event Management (SIEM). Considering the wide area of information available and the multiple available sources, we propose integration of the data and information using fusion tools, with the end goal of obtaining synergy. The corpora of fused information will be described through semantics and will be usable in the other information processing and exploitation methods.

Figure 3 illustrates the EnergyShield's data processing strategy emphasising the data fusion. The data processing is organized into four steps.



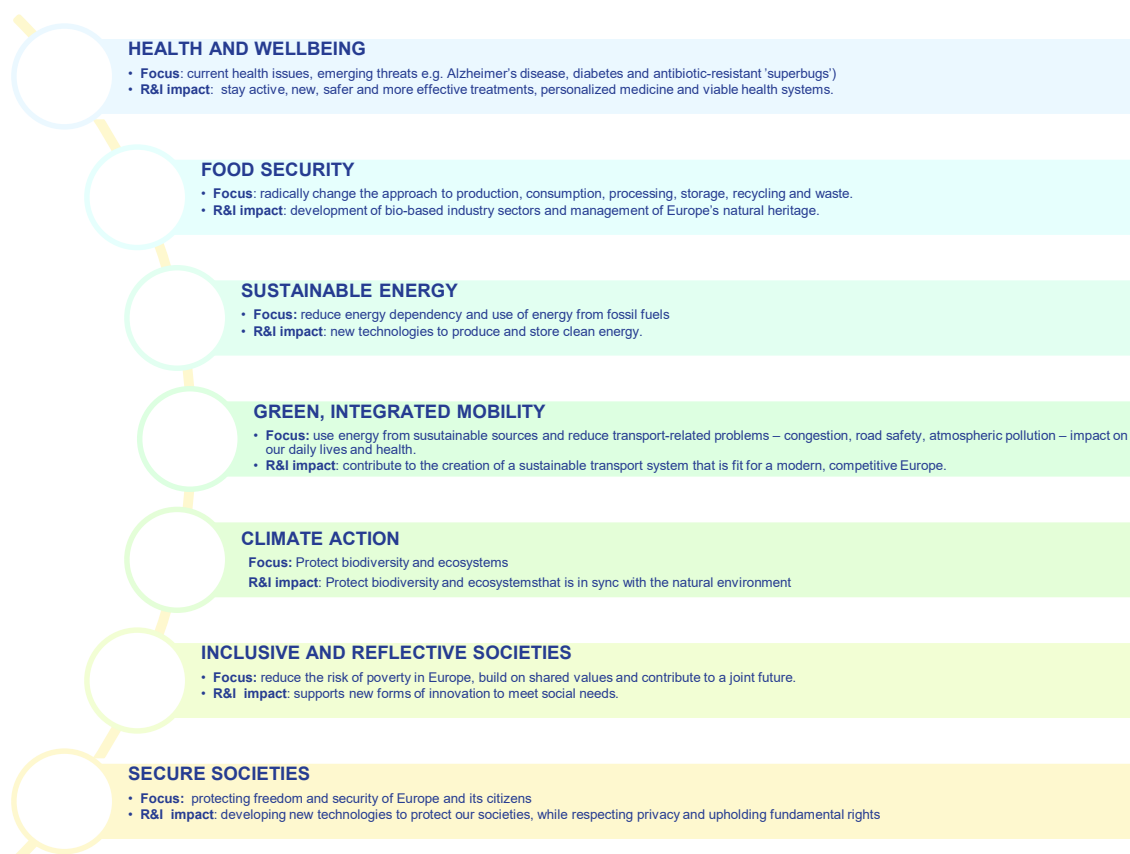
**Figure 1. Semantic fusion and classification**

## 2.1. RESEARCH AND INNOVATION CHALLENGES

Research and Innovation (R&I) projects are the main drives to achievements in science and technology. Under the specific programme implementing Horizon 2020, Societal Challenge 7 “Secure societies – protecting freedom and security of Europe and its citizens” concerns the research and innovation activities needed to protect our citizens, society, and economy as well as our infrastructure and services, our prosperity, political stability, and wellbeing. [PAS16]

- Health, demographic change, and wellbeing
- Food security, sustainable agriculture and forestry, marine and maritime and inland water research, and the bioeconomy
- Secure, clean, and efficient energy
- Smart, green, and integrated transport
- Climate action, environment, resource efficiency and raw materials
- Europe in a changing world – inclusive, innovative, and reflective societies
- Secure societies – protecting freedom and security of Europe and its citizens.

Figure 2 summarises the focus of societal challenges and impact of R&I investments.



**Figure 2. Focus of societal challenges and impact of R &I investments**

The impact of the R&I investments and, consequently the scientific advancements and the deployment of new concepts and technologies is positive in the society in general. However, technological development and social needs need to be matched.

## 2.2. ENERGY LITERACY PRINCIPLES

CLEAN (Climate Literacy and Energy Awareness Network) [CLE22], a U.S. foundation sponsored by the National Oceanic and Atmospheric Administration, the National Science Foundation, the Department of Energy, and NASA, defined 6 key concepts as part of what they call energy literacy depicted in Figure 3.



**Figure 3. The key concepts of energy literacy [CLE22]**

Details about each concept of energy literacy are provide below; :

- **Economic security is impacted by energy choices.**

Economic wealth is sometimes associated with the consumption of energy and the average number of electronic and electric powered devices per capita. The concept is based on the presumption that the more energy consumed the more evolved the society is because the devices using the energy help individuals (and by extension society) to develop new things and also by replacing human effort. With evolution more demands come not only in energy consumption but with energy interconnection and smart grid evolution, which means more and more internet access that increases the demand for cyber security tools to protect the grid.

- **National security is impacted by energy choices.**

The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. If the nation is dependent on foreign energy, it might be destabilised by an unexpected disruption in the supply chain. Grid resilience is very important, especially in case of cyber-attacks.

- **The security of a nation is dependent, in part, on the sources of that nation's energy supplies.**
- **Increasing demand for and limited supplies of fossil fuels affects quality of life.**

There is a clear direction for most nations, to use clean energy as much as possible and cut dependence on fossil fuels. The use of renewable energy means a constant integration with various smart devices and SCADA systems which translates into interconnected online system that processes vast amounts of real time data from

multitude of sensors. All these requirements lead to one thing: the need for integrated cyber security toolkits in the design of the grid.

- **Access to energy resources affects quality of life.**

Energy is related to all walks of life: we need energy for air condition, entertainment, communication, home office, food cooling, automatic sliding doors, digital payment, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society.

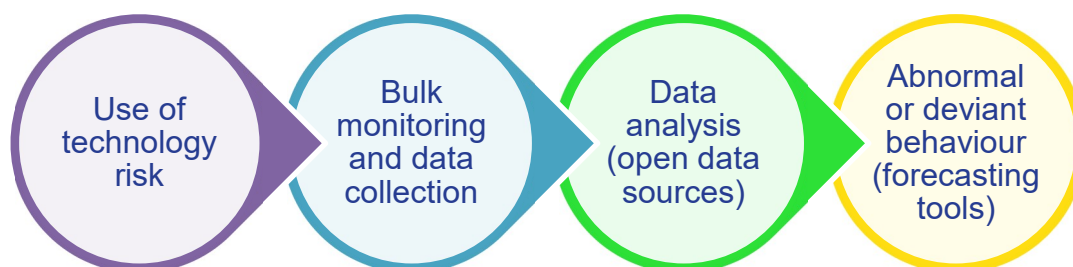
- **Some populations are more vulnerable to impacts of energy choices than others.**

All decisions regarding the production and use of energy have economic, social, and environmental consequences. Poor, marginalised, or underdeveloped populations benefit the most from the positive consequences of the use of energy, but also can be impacted more by the negative consequences.

## 2.3. SOCIETAL “FACE” OF CYBER-ATTACKS

Cyberattacks are defined here as events which aim to compromise the integrity, confidentiality, or availability of a system (technical or socio-technical). These attacks range from hacking and denial-of-services (DoS) to ransomware and spyware infections and can affect everyone from the public to the critical national infrastructure of a country [NUR18].

The topic of cyber-attacks has a social component and may also have behavioural impact. Figure 4 provides an overview of risks and impacts raised by the objectives and the core concept of the technology being developed in the EnergyShield project.



**Figure 4. Societal impact of using technologies and methods**

- Societal risks envisioned using certain tools and methods

The ever-extended use of technology also reaches users that lack an IT&C literacy. Thus, the risk of becoming a cyber-attack victim is high and raises difficulties in building an effective manner to react to those attacks. Thus, the perception of risk may be altered and/ or the reaction may be emotional or submissive (accepting risk exposure or being a victim due to lack of knowledge).

- Bulk monitoring and data collection (“analysing and jointly exploiting multiple massive data streams”)

**Bulk monitoring** is a problem when the data is used as surveillance. It typically starts from suspicion about the criminal activities of an individual or several individuals (insider threats), and then collects various sources of information, intelligence, or evidence about them. In contrast to this, mass surveillance considers a much wider range of information sources when attempting to identify unknown dangers or threats [COE17]. Engaging in mass surveillance generally includes information gathering on many people who would not normally be considered a threat or placed under police surveillance. Bulk monitoring, therefore, elevates many people into the realm of being potentially suspicious. In such circumstances, suspicion does not precede data collection, surveillance is not initiated based on ‘reasonable suspicion’. Rather, it is generated by analysis of the data itself [FUS19].

**Conducting bulk data collection** makes it difficult to ascertain who the data subject is. Bulk monitoring has a “chilling effect” (individuals refrain from engaging in certain forms of activity because of the perceived consequences if that activity is observed) [SOL06]. Individuals may refrain from lawfully exercising their democratic rights due to a fear of the consequences that may follow. Existing research indicates that those most vulnerable to a chilling effect are opposition movements, minority groups and those with the fewest resources to challenge the status quo [FUS19]. The effect is such that bulk monitoring may reproduce marginalisation and impact upon, or undermine, the basis of a pluralistic democracy, that is, the ability to debate and oppose government policies.

**Widespread interference** with the right to privacy, freedom of expression, association and assembly may have implications both at the individual level, affecting individuals’ ability to freely develop their identity and opinion, and at the societal level [FUS19]. The constant feeling of being observed can cause deep mistrust of authorities by citizens, which could result in self-censorship and change of behaviour.

- Analysing data coming from open sources such as: online social networks, the open web, the darknet

Although OSINT (*open-source intelligence*) indicates that all the data collected through these techniques is publicly available, it still challenges privacy and ethical principles. One of the key questions related to the ethical dilemmas of social network analysis is the extent to which data ought to be considered private or public. We can assume (hopefully) that service providers and data controllers have informed users

in their terms and conditions that their data might be used by third parties, e.g., other companies, or for the purpose of research.

In the case of big data analysis, there is an ingrained temptation to collect and process as much data as possible, which cannot be reconciled with the data minimisation principle and purpose limitation [SCH15].

Bringing together and processing different data sets reveals more information about individuals than processing them separately, which is difficult to anticipate at the time when data is shared by data subjects. This challenges the principle of consent to data processing, as it is defined and presented in [MAY13].

No dataset can perfectly describe a network (community), as it is difficult to represent the true size, number of members, who those members are, and the quality of relationships between them in a dataset [LIK13].

- Predicting abnormal or deviant behaviour

**Machine learning (ML) and Artificial Intelligence (AI).** Mathematical models or algorithms claim to quantify important traits, but the systems may have harmful outcomes and reinforce inequality. Machine learning and use of AI might “hardwire” a system based upon faulty, historical data that may reflect racial or ethnic disparity characterised by increased rates of stop and search, prosecution, punishment, and imprisonment for minority groups and communities when compared to the majority population. It may perpetuate pre-existing human biases and social inequalities (risk of “weapons of math destruction”) [ONE16].

Models might be affected by the norms, values, and assumptions of their developers.

The models are often proprietary, so they have the effect of being a black box (lack of transparency). They affect large numbers of people, increasing the chances that they get it wrong for some of them.

Automated processing can make external assessment of the system complicated and difficult for users and data subjects to understand or to challenge the process (the problem of explainability). It may be hard for users to identify if the system is not working properly, or to diagnose reasons for failure.

The proliferation of algorithmic decision making might undermine the skill and decision-making activities of professionals, placing over reliance on information provided by technology (the “autopilot problem”).

Bias/arbitrariness in deciding what kind of behaviour is considered “deviant” or “abnormal” based on “measurement error and/or representation error”. Measurement error refers to how accurately the data used indicate or reflect what is intended to be measured. For machine learning systems, measurement error links to the question of which features are included in the training data, i.e. is the information that is intended to be analysed amenable to being measured well, and should it be used to predict outcomes? Representation error links to the question of how representative a sample is of the population [EUA19].

There is often a lack of clarity as far as the following questions are concerned:

- a) Does the public know **who** is using their data?
- b) Do they know **how** it is being used?

- c) Do people know how to **access** the resources related to machine learning?
- d) Where can they **opt in/out** of their data being used for ML? It has been argued that for ML tools to be ethical, the people whose data is being used for training the models should **at least** be allowed to **remove** themselves from the models, express a wish not to be used in the model in the future, etc.
- e) It is also important that machine learning allows us to extract information from data and discover new patterns and can **turn seemingly innocuous data into sensitive, personal data**. This has significant repercussions for privacy and anonymity, both online and offline. It is worth noting as well that although there are several laws aimed at protecting the privacy of people, such as the General Data Protection Regulation (GDPR), they apply to personal information. The aggregated data which is used to train models is “anonymous” and thus the laws may not apply here.

In some countries sentiment analysis tools have been deployed specifically to control the tone and nature of online comments. Sometimes, they have been trained to remove content in an automated way. This risks censorship and violate freedom of speech. In addition to this, ML-based internet surveillance may encourage self-censorship and thus lead to one's freedom of expression being affected. Additionally, there have been the concerns about AI-powered technologies being used to manipulate people, e.g., by autonomous social media accounts, spreading propaganda and fake news before elections and voting. The result of them bombarding the internet with this kind of content is manipulating public opinion; sometimes even by harassing the social media users who criticise the government. AI has also been used to target, profile, and manipulate individuals. Similarly, algorithms have been used by the media outlets to show customised news to citizens, based on the stories they read before. This leads to the so-called “filter bubbles”, i.e., people not being presented with new standpoints and ideas and being exposed only to opinions they share. This may disrupt the principles of democracy.

Finally, there are the questions of **responsibility for the actions of an algorithm**. Who should be responsible for them – the developers, end users or the AI itself? Based on the current laws in Europe, as a rule, the responsibility for AI's actions is attributed to humans: for example, its operators or owners. Then, what if the AI learnt to such an extent that it has changed from its original design? Is it still the programmer's liability?

**Use of forecasting tools.** Predictive systems rely on historical data held by the entity using the tools, which can contain bias.

The accuracy of the prediction is tested against the (potentially biased) historical data and therefore is not an objective baseline.

The belief in the objectivity of historical data may cause an over monitoring of a situation that doesn't need it.

There is a risk of the lack of transparency from both public and private entities regarding how predictive models are built, how the data and whether the programs unnecessarily target specific user groups more than others.

A RUSI (Royal United Services Institute) briefing paper offers a summary of some of the available empirical evidence regarding the effectiveness and accuracy of predictive policing technology. In summary: high accuracy rates at the group level can often conceal very low accuracy rates for specific individuals or groups of individuals within that larger group. All individual predictions are associated with a confidence interval (a margin of error), which is often not considered when reporting the overall ‘predictive accuracy’ of the tool [BAB19]. The above-mentioned problem, though specific to algorithms used by police in mass surveillance, applies to other domains too.

One expert interviewed for the RUSI briefing paper pointed out that “there are a lot of myths around machine learning tools and what they can do. One of the things that machine learning is not proficient on is predicting rare and infrequent events, especially when you don’t have loads of data.” As summarised by Alan A. Sutherland and colleagues, “predictive judgments are meaningful when applied to groups of offenders. However, at an individual level, predictions are considered by many to be imprecise” [SUT12]. The above-mentioned problem, though specific to algorithms used by police in mass surveillance, applies to other domains too.

## 2.4. PROPOSED APPROACH

The process of the ethical, legal and societal impact assessment builds on and elaborates the concept of privacy impact assessment (PIA). PIA is a methodology for assessing the potential impacts on privacy of a project, policy, programme, service, product or other initiative and, in consultation with stakeholders, for taking remedial actions as necessary in order to avoid or minimise negative impacts. It is a tool to undertake the systematic analysis of the project in order to inform decision-makers and mitigate the risks (using the term in a wide sense) [WRI12]. PIA has been referred to as an *early warning system*, as it provides a way to detect potential problems, take precautions and introduce mitigation measures early in a process. PIA acts as a foundational component for achieving “privacy by design”. Over the years, PIA has been gaining traction as an important instrument for protecting personal data and privacy [WRI13]. The Madrid Resolution adopted by the International Conference of Privacy and Data Protection Commissioners in November 2009 encourages “the implementation of privacy impact assessments prior to implementing new information systems and/or technologies for the processing of personal data, as well as prior to carrying out any new method of processing personal data or substantial modifications in existing processing” [WRI09].

Generally, if the development and deployment of a new project (or technology, service, policy or other initiative) impacts upon privacy, a PIA should be conducted. Different impact assessment methodologies have expanded in several directions complementary to PIA, including ethical impact assessments [WRI15a], surveillance impact assessments [WRI15b] and societal impact assessment [WRI15c].

Building on these developments, the aim of an integrated ethical, legal, and societal (ELS) impact assessment is to identify and assess the potential impacts of a project (or a policy, programme, service, product, or other initiative) and, in consultation with stakeholders, to recommend solutions and remedial actions necessary in order to avoid or minimise negative impacts. An ELS impact assessment spans through the

lifecycle of a project from the early design to the deployment of the product and service.

While this report focuses on the societal impact assessment the ethical and legal aspects are approached in D1.6 [ESH16].

The overall purpose of the societal assessment in EnergyShield is to:

- identify societal impact of the project, including the risk of misuse of research results;
- assess the risks (likelihood and seriousness of possible impacts);
- outline mitigation measures and their implementation status;
- make recommendations for the deployment of EnergyShield-like systems.

To address these objectives, a template was prepared and submitted to technological partners. The aim of this survey is to identify the drivers and factors within EnergyShield tools that could have a societal impact.

**Table 1. Survey to identify the social impact of EnergyShield**

<b>Name of the tool</b>	<b>&lt;name&gt;</b>
<b>Leading partner</b>	<name>
<b>Contributing partners</b>	<name>
<b>Tool type</b>	<i>Assessment / Monitoring / Supervision</i>
<b>Tool description including algorithms that have a societal impact</b>	<i>&lt;add details about the features, functionalities, algorithm that have a societal impact&gt;</i>
<b>Identified societal issues</b>	<i>&lt;provide details about the personally identifiable information (PII) stored by the tool&gt;</i>
<b>Security requirements implemented in the tool</b>	<i>&lt;list the security requirements and technologies deployed&gt;</i>
<b>Risk mitigation methods implemented by the tool developer</b>	<i>&lt;please provide details about deployment on premises&gt;</i>
<b>Adhere to the 6 principles of energy literacy</b>	<i>&lt;evaluate how the tools adheres to the 6 energy literacy principles:</i> <ul style="list-style-type: none"> <li>- <i>P1 – Economic</i></li> <li>- <i>P2 – National security</i></li> <li>- <i>P3 – Environmental quality.</i></li> <li>- <i>P4 – Demand and quality of life.</i></li> <li>- <i>P5 – Access &amp; quality of life</i></li> </ul>

	- P6 – Impact of energy to populations >
--	--

### 3. SOCIETAL IMPACT OF ENERGYSHIELD TOOLS

In this section, we discuss issues raised by EnergyShield tools and toolsets. For each tool, a brief description, an outline of the Societal Impact Assessment (SIA) the tool raises and how they have been addressed is provided.

#### 3.1. SOCIETAL IMPACT ASSESSMENT (SIA) OF TOOLS

##### 3.1.1. SIA OF VA TOOL

**Table 2. Societal impact assessment of VA tool in the EnergyShield project**

Name of the tool	Vulnerability Assessment (VA)
<b>Leading partner</b>	Foreseeti AB
<b>Contributing partners</b>	KTH for final document review
<b>Tool type</b>	<b>Assessment</b>
<b>Tool description including algorithms that have a societal impact</b>	<p>The Vulnerability Assessment tool is based on Foreseeti's securiCAD Enter-prise product – a system for analysing cyber threat exposure by means of threat modelling and attack simulations. The development of the VA tool has been entirely possible to include in securiCAD Enterprise, making it capable of performing the role of the VA tool with only minor extensions to the standard product packaging.</p> <p>There are multiple benefits of the VA tool:</p> <ul style="list-style-type: none"> <li>• It allows working with security holistically at a scale and frequency un-attainable by manual analysis</li> <li>• It gives a repeatable, low-bias way of quantifying cyber resilience, thereby allowing baseline measurements against which deviations can be tracked</li> <li>• It is non-intrusive, meaning it will not interfere with the actual systems – something that is particularly valuable in sensitive SCADA environments typically found in the EPES domain.</li> <li>• Allows for cost effective and continuous analysis</li> </ul> <p>The goal of the VA tool is to assess the cyber security resilience through threat modelling and attack simulations. It assumes a completely rational at-tacker with full insight to all attack opportunities. In short, there are three steps to an analysis:</p>

	<p>Create model -&gt; Simulate attacks -&gt; Evaluate the analysis results</p> <p>After the model is created the VA tool will generate a report that has the following information:</p> <ul style="list-style-type: none"> <li>• Total risk exposure - a consequence-weighted risk across all high-value assets.</li> <li>• The number of high value assets at risk/reached within the cut-off time horizon (default is 100 days).</li> <li>• The total number of assets in the model.</li> <li>• The total number of associations in the model (connections between modelling objects).</li> <li>• The number of attack steps included in the automatically generated at-tack tree that the simulation engine is using for this model.</li> <li>• The number of applied defences and defences that can be enabled at the modelling objects related to the expected attack paths.</li> <li>• The number of attack operations that an attacker is expected to use along the attack paths from the starting point to the high-value assets.</li> <li>• The number of suggested mitigations found in the model, based on the attack simulations.</li> </ul>
<b>Identified societal issues</b>	<p>The tool doesn't store many PII's, except those needed to create an account such as email, organisation, name. The tool has a societal impact since it helps secure the EPES value chain. The information contained in the tool about the EPES infrastructure is very important.</p>
<b>Requirements implemented in the tool</b>	<p>The tool was designed to function in high security environments and uses https only and logged-in sessions for both users and SDK. We have deployed the following:</p> <ul style="list-style-type: none"> <li>• Langpacks- A new format has been created for MAL domain support packages that include both MAL based language JARs as well as Docker-based parsers. Running parsers in containers is an important step up in system security as the container isolation gives a high degree of protection of the VA tool integrity.</li> <li>• JSON - logging System logs are now formatted as highly structured JSON objects to support easier post-processing.</li> </ul>

	<ul style="list-style-type: none"> <li>• Red Hat / CentOS support - Added support for Red Hat Enterprise Linux/CentOS 7 &amp; 8</li> <li>• Offline installation - Support installations without Internet access (standard installation will download packaged from OS repos) as required in some high-security environments and preferred by operators of critical infrastructures, supporting both Ubuntu and RHEL/CentOS.</li> <li>• Nginx security configuration - Strengthened HTTP headers security configuration of the nginx reverse proxy in the VA.</li> <li>• EnergyShield branding - Branding package for EnergyShield, with project logo and colour scheme.</li> <li>• Remove dependency on the EPEL - Optimised package dependencies to avoid reliance on the “non-standard” EPEL repo for RHEL/CentOS.</li> <li>• Upgrade refactoring - Increased robustness for system upgrades, removing dependency on the ORM database layer.</li> </ul>
<b>Risk mitigation methods implemented by the tool developer</b>	<p>Care has been taken to develop a product packaging that allows deployment and use in shifting environments, ranging from on-site deployment in high-security environments without Internet access to the ability to deploy the product as a multi-tenant Software as a Service (SaaS) tool. In the energy sector, many grid operators or generation plant operators are rated critical infrastructure operators and have a high preference for on-premises deployment.</p>
<b>Adhere to the 6 principles of energy literacy</b>	<p><i>This tool helps with all the 6 principles of energy literacy:</i></p> <ul style="list-style-type: none"> <li>- P1 – Economic security – security tools are needed more than ever because of the needs for more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> <li>- P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>- P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>- P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection</li> </ul>

	<p>and Internet access which translates in the need for better security tools.</p> <ul style="list-style-type: none"> <li>- P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use: air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> </ul> <p>P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The interconnected grid needs to have security tools implemented from the design phase.</p>
--	--

### 3.1.2. SIA OF SBA TOOL

**Table 3. Societal impact assessment of SBA tool in the EnergyShield project**

Name of the tool	Security Behaviour Analysis (SBA)
Leading partner	NTUA
Contributing partners	Foreseti,
Tool type	<b>Assessment</b>
Tool description including algorithms that have a societal impact	<p>The objectives of this tool are to:</p> <ul style="list-style-type: none"> <li>• perform the assessment of the security culture of an organisation at different levels (organisation, department units, and employees),</li> <li>• map the socio-cultural behaviour of end-users to specific cyber-threats,</li> <li>• provide insights for decision-making regarding improving the security culture of the company,</li> <li>• assist in planning and implementation of security culture training programs.</li> </ul> <p>The results of the SBA tool assessments are further communicated to the EnergyShield Vulnerability Assessment tool via Kafka messages and the REST API, showing the effect of user's cyber awareness and skill in a holistic security context. The Security Behaviour Analysis tool has been integrated with the overall EnergyShield toolkit and is currently validated by the pilot users in the EPES sector.</p>

	<p>The tool can measure the following insider threats factors:</p> <ul style="list-style-type: none"> <li>• Dissatisfaction</li> <li>• Personality predispositions</li> <li>• Enterprise role</li> <li>• Concerning behaviour</li> <li>• Employee profile</li> <li>• Access Controls</li> <li>• Sense of entitlement</li> <li>• Policy violation</li> <li>• Auditing</li> <li>• Policies and roles awareness</li> <li>• Situation awareness</li> </ul>
<b>Identified societal issues</b>	<p>Though the attack methods vary depending on the industry, they have identified, analysed, and presented via several technical reports the main insider threat types and their subcategories, as a part of the Management and Education of the Risk of Insider Threat (MERIT) project:</p> <ul style="list-style-type: none"> <li>• Information Technology (IT) Sabotage: Use of IT to direct specific harm toward an organisation or an individual.</li> <li>• Intellectual Property (IP) Theft: Purposely abuse one's credentials to steal confidential or proprietary information from the organisation.</li> <li>• Entitled Independent: An insider acting primarily alone to steal information to take to a new job or their own side business.</li> <li>• Ambitious Leader: A leader of an insider crime who recruits insiders to steal information for some larger purpose.</li> <li>• Fraud: Unauthorised modification, addition, or deletion of an organisation's data for personal gain, or theft of information that leads to an identity crime (e.g., identity theft, credit card fraud).</li> <li>• Espionage: Obtaining, delivering, transmitting, communicating, or receiving information about the national defence with an intent, or reason to believe, that the information may be used to the injury of one's country or the advantage of any foreign nation.</li> </ul>

	<ul style="list-style-type: none"> <li>Unintentional Insider Threat (UIT): Negatively affect the confidentiality, availability, or integrity of an organisation's information or information systems via action or inaction without malicious intent.</li> </ul>
<b>Requirements implemented in the tool</b>	<p>The Security Behaviour Analysis (SBA) tool has been designed, developed, and implemented as a web application using several cut-edge technologies. Specifically:</p> <ul style="list-style-type: none"> <li>Django: a high-level open-source Python Web framework that encourages rapid development while offering the ability to quickly and flexibly scale. Its security features enforce applications' protection against common security issues, such as SQL injection, cross-site scripting, cross-site request forgery and clickjacking.</li> <li>PostgreSQL: a powerful, open-source object-relational database system with a strong reputation for reliability, feature robustness, and performance. It is used to host the logical data structure behind the entire application, including the security culture model and the representation of the evaluation methodology, along with its results and statistics.</li> <li>Web interface: implemented using a combination of HTML, Bootstrap, CSS and JavaScript files to provide a user-friendly interface for all interacting actors of the tool.</li> <li>REST API: a web interface allowing interaction of the SBA tool with the rest of the EnergyShield toolkit or with any other corporate operational system.</li> <li>Kafka Producer: a Kafka client publishing messages to specific Kafka topics to inform listening parties (Kafka consumers) that new evaluation data have become available (e.g., at the end of an assessment campaign).</li> </ul>
<b>Risk mitigation methods implemented by the tool developer</b>	<p>Anonymisation - As with every corporate assessment tool dealing with personal data, our CSC framework, reaching down to an individual level, conforms with all regional and international laws protecting human's privacy. Therefore, our tool ensures compliance with the European Data Protection Regulation (GDPR) meaning properly informing employees and ensuring their written consent prior to campaign participation while offering anonymisation possibilities which</p>

	<p>can be enabled or disabled based on organisation needs and policies.</p> <p>Thus, SBA contributes to understanding individual security risks and training needs, discomfort from demanding and inapplicable policies, and difficulties deriving from working security routine. In other words, SBA accommodates the working force by retrieving security gaps, pinpointing policy complexity and, finally, facilitating participation in cyber-security defence. Using the anonymisation feature, ensures that SBA is not being used as a rating mechanism and an employee competency guide since working abilities and professionalism do not always go hand-by-hand with information security awareness. Security professionals and officers need to safeguard its role and usage, as with all security infrastructure, and to guide users through a prosperous exploitation.</p>
<b>Adhere to the 6 principles of energy literacy</b>	<p>This tool helps with all the 6 principles of energy literacy:</p> <ul style="list-style-type: none"> <li>• P1 – Economic security – security tools are needed more than ever because of the needs of more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> <li>• P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>• P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> <li>• P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The</li> </ul>

interconnected grid needs to have security tools implemented from the design phase.

### 3.1.3. SIA OF AD TOOL

**Table 4. Societal impact assessment of AD tool in the EnergyShield project**

Name of the tool	Anomaly Detection
Leading partner	SIGA
Contributing partners	CITY, SIMAVI final document review
Tool type	<b>Monitoring &amp; protection</b>
Tool description including algorithms that have a societal impact	<p>This anomaly detection tool is based on the solution and technology developed by SIGA OT Solutions. SIGA's solution is a comprehensive process anomaly detection system that monitors critical assets using ICS/SCADA electrical signal-based advanced analytics, Artificial Intelligence and Machine Learning.</p> <p>This tool monitors and analyses the OT level 0 part of the different EPES assets that will be connected to the EnergyShield solution. The tool is duplicating unidirectionally the asset's ICS/SCADA electrical signals, which runs between sensors and actuators to the PLC, and is performing real-time process-oriented anomaly detection by using algorithmic models on this data to detect and alert on abnormal behaviour of the process, indicating on a potential on-going cyber-attack on the asset.</p> <p>The is out-of-band, separate and independent from the asset's ICS. It is providing real-time reliable status of the assets, sending anomaly alerts and actionable insights to the EnergyShield SIEM and to any other system required. It is also providing the user with an independent smart dashboard (GUI) for visibility, alerts, and analysis.</p> <p>The tool is based on SIGA's holistic and unique approach aiming to fully utilise the distinguished attributes and qualities of directly extracted critical process information at level 0, coupled with proprietary process-oriented Machine Learning models to enhance OT cyber security and process optimization for operators. The tool is automatically and autonomously learning the normal behaviour of the asset's</p>

	<p>industrial process for a limited time (called “learning period”), and once it is over, the solution is searching for abnormal behaviour, therefore detect anomalies when they occur.</p>
<p><b>Identified societal issues</b></p>	<p>ICS/SCADA used to be considered as safe from cyber-attacks because they are isolated and air-gapped networks. However, these critical systems are extremely vulnerable. The development of the Industrial Internet of things (IIoT) and the convergence of OT and IT networks are creating a perfect environment for hackers to attack highly attractive targets – operational processes. Recent deliberate disruptions of critical automation systems prove that cyber-attacks can have disastrous consequences for citizens and nations. Malicious code can potentially be used to manipulate the controls of (among others) power plants, HV sub-stations, LV sub-stations etc. All of these are considered critical infrastructure with damage potential resulting in real-world catastrophic physical damage, such as blackouts and substantive threat to human lives.</p> <p>The transition to Industry 4.0 requires IT/OT convergence and accelerated “connectivity”, combined with the global cybersecurity challenge – the Unknown Unknowns, and the ever-growing frequency &amp; magnitude of cyber-attacks, raise new concerns and potentially disastrous consequences: financial losses, regulatory breaches, reputational damage, lawsuits, management liability, high remedial costs &amp; risk to health.</p> <p>The most critical layer of the OT is the “Physical layer”, or “level 0”, which is exposed to cyber-attacks of any man-in-the-middle type of attack, like “Stuxnet” or “Irongate”, or to supply chain attacks like “SolarWinds”, “Aurora” and basically any type of attack that is trying to manipulate the process and cause physical damage.</p> <p>Today, all available ICS cybersecurity solutions are based on securing the IP-based network (Data packets), starting from the PLCs, Level 1 of the Purdue Model, and moving up the network to supervisory controls, operations management, and business management. Of course, securing the data-network is crucial, however, it can be hacked despite the layers of protection installed and the operators don’t even know it. The assets themselves, the operational processes stay vulnerable and the attacks on these assets stay hidden and unseen.</p> <p>The AD tool solves this challenge by monitoring the physical source of information, which cannot be hacked – the raw electrical signals of level 0 – sensors and actuators. The</p>

	<p>ICS/SCADA electrical signals at LEVEL 0 are the most reliable source of data for OT environments, it is rich &amp; unfiltered, unhackable, and often un-available to operators.</p> <p>By activating ML detection engine on the reliable, rich, and unfiltered electrical signals at Level 0, the tool delivers autonomous cyber inspection &amp; analytics solutions, offering bullet-proof detection of any cyber-attack on the physical layer, inaccessible insights, and operational resilience of industrial processes and automated machinery.</p>
<b>Requirements implemented in the tool</b>	<p>The tool integration capabilities are:</p> <ul style="list-style-type: none"> <li>• The tool uses high resolution measurement of the ICS/SCADA electrical signals, to provide granular information of the process, therefore enabling high visibility into the process.</li> <li>• The tool is hard-wired into the control loops without having any impact or interference to the ICS/SCADA operation, duplicating the electrical signals unidirectionally into the tool data collection mechanism.</li> <li>• The tool input interface is only a measurement of the electrical signals and not connected at all to the PLCs or the OT network, hence it is totally agnostic to the ICS/SCADA equipment (manufacturer, model etc.) and to communication protocols.</li> <li>• The tool is very flexible and agile, and it can be installed and operated based on the monitored systems owners' requirements.</li> <li>• The tool's basic output (i.e., its interface with the user), will be through visualisation, alerts, analyses and reports in the tool's dashboard (GUI). The tool can also send alerts, messages, and reports via multiple channels, e.g., e-mail, SMS, SYSLOG, JSON, API integration etc.</li> <li>• The installation is easy, simple, and fast and can be performed by any ICAS/SCADA technician.</li> </ul>
<b>Risk mitigation methods implemented by the tool developer</b>	<p>The AD tool is a breakthrough in OT cyber protection, providing safety for industrial assets by directly monitoring raw electrical signals (level 0 real-time monitoring) – while other cyber security solutions are part of the ICS network (IT, data packets that can be “hacked”). This tool brings unmatched visibility into physical processes, to support</p>

	<p>intelligent, real-time action, enhanced by diagnosis and AI, empowering operators with timely alerts and actionable insights.</p> <p>SIGA's core solution is based on securing raw data duplication, based on fully out-of-band hardware, reliable encrypted data delivery, and multi layered analysis aiming to identify process abnormalities caused by cyber-attacks. By utilising this unique data source to deliver reliability and cyber security protection, SIGA's AD tool has several main advantages:</p> <ul style="list-style-type: none"> <li>• Process-oriented anomaly detection, focuses on the core critical assets, the operational process, and not on the information layers above it</li> <li>• Operational Reliability &amp; Situation Awareness through Electrical Signal Monitoring from untampered and unavailable (0,1) level, hence totally out-of-band and protocol agnostic</li> <li>• Real-Time OT sensors and process analytics for monitoring &amp; detection</li> <li>• A single source of Unfiltered, AI &amp; ML Analysis and actionable data, enabling task-specific, business-critical modules that minimise risk and generate value</li> <li>• Inherent OT Cyber Security – Based on a separate, independent network, independent from the monitored asset's ICS/SCADA</li> </ul>
<p><b>Adhere to the 6 principles of energy literacy</b></p>	<p>This tool helps with all the 6 principles of energy literacy:</p> <ul style="list-style-type: none"> <li>• P1 – Economic security – security tools are needed more than ever because of the need for more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> <li>• P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>• P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection</li> </ul>

	<p>and Internet access which translates in the need for better security tools.</p> <ul style="list-style-type: none"> <li>• P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> </ul> <p>P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The interconnected grid needs to have security tools implemented from the design phase.</p>
--	---

### 3.1.4. SIA OF DDoSM TOOL

**Table 5. Societal impact assessment of DDoSM tool in the EnergyShield project**

<b>Name of the tool</b>	<b>Distributed Denial of Service Mitigation (DDoSM)</b>
<b>Leading partner</b>	L7 Defense
<b>Contributing partners</b>	KT, CITY, SIMAVI for final document review
<b>Tool type</b>	<b>Monitoring &amp; protection</b>
<b>Tool description including algorithms that have a societal impact</b>	<p>The smart grid is a unique system consisting of many overlaid and interdependent components and processes. Specifically, it is made up of the IT (information) and OT (operational) technology networks, which work together for dynamic monitoring and control. This interaction means that failures in the IT network can lead to a wider disruption. Furthermore, given the nature of electrical energy, maintaining grid-wide stability and synchronisation is required. This means that disruption to IT data flows can again lead to wider disruption.</p> <p>DDoS attack aimed to degrade services SLA (availability). As IT component operations rely on services (APIs) communication, it needs to be protected from this type of threat. Such a protection is the purpose of the DDoSM tool. This section describes the DDoSM's core concepts, the methodology employed, the Ammune framework, the analytical models, and a summary of the project defined KPIs.</p>

	<p>To generate a substantial and effective DDoS flood botnet is typically employed, aiming for sheer numbers or for complex low-and-slow style crafted messages. It provides the necessary number of geographically distributed endpoint bots, as well as automation (via "command-and-control" channels) needed for attack synchronisation. The botnet DDoS activity may simulate external sources of attack or ones that are created within the AMI from corrupted smart metres. The DDoSM tool consists of Ammune, placed in-front of vulnerable IT components while protecting from incoming attacks. Ammune's AI-driven system is bolstered by analytical models capturing the key components of a DDoS attack, as well as the dynamics of a spreading wave of compromise - triggered by the attack – through the grid networks. Ammune AI machinery builds a dynamic protection profile and policy for each active API endpoint through in/out traffic inspection.</p>
<b>Identified societal issues</b>	<p>Ammune algorithms were retrained and recalibrated to better handle smart grid scenarios and to offer EPES resilience to cyber-attacks:</p> <ul style="list-style-type: none"> <li>• Ammune DDoS detection was recalibrated and relearned to better handle extra heavy-duty calls, which could be abused at extremely low rate. Ammune detection was less efficient at DDoS that sufficiently overloaded systems at rates below 10 req/sec. The algorithm was recalibrated to enable successful DDoS detection at rates above 1 request per second.</li> <li>• Ammune DDoS detection was recalibrated to add a significant weight to calls returning error. It increased sensitivity for capturing attacks that overload systems with calls to non-existent objects thus bypassing cache.</li> <li>• Ammune analysis time slot was reduced from 5 to 1 second, with a goal of reducing the attack mitigation time, thus reaching the KPI of under 1 minute attack mitigation in 98% of DDoS attacks.</li> </ul>
<b>Requirements implemented in the tool</b>	<p>L7 Defense's Ammune™ API security solution is an advanced AI solution based on unsupervised ML. It protects APIs from advanced attack types, with a minimal impact on the legitimate traffic. It automatically discovers and protects each API separately. Ammune continuously builds a specific profile (an AI baseline) for each API, which is used to spot and stop emerging threats that otherwise go unnoticed, in real time, and without any prior knowledge or signatures of the attack</p>

	<p>characteristics. It is inspired by the "innate immune system" model, designed for accuracy, minimises the damage from both erroneous detection (false positives) and from incoming attack penetration (false negatives).</p> <p>Ammune protects financial services, e-commerce, critical infrastructure, and other organisations from advanced AI-driven cyber-attacks.</p> <p>Ammune contains the following functional modules:</p> <ul style="list-style-type: none"> <li>• API-WAF protecting from content injection threats targeting remote command execution, data exfiltration, denial of service and more.</li> <li>• API-BOT protecting from advanced automated threats that implement data exfiltration, fraud actions, account takeover, functionality abuse and more.</li> <li>• API-DDoS protecting from DDoS attacks on API business logic that attempt to overload computation and memory resources of the application servers.</li> <li>• API-BL protection on API from business level exploits, such as authorization and authentication bypasses.</li> </ul>
<p><b>Risk mitigation methods implemented by the tool developer</b></p>	<p>At its core Ammune is built to support protection against API attacks as well as analytics. Hence its architecture is built of two parts: real time traffic enforcement unit and analytics unit that provides near real time analytics of the traffic flows.</p> <p>Ammune supports various embedding architectures:</p> <ul style="list-style-type: none"> <li>• Network TAP - copy of the traffic is received in Ammune Real-Time module directly from network tap (without reverse proxy). In this case Ammune real time can't implement mitigation but blocking commands could be send to other enforcing devices.</li> <li>• Log feed - copy of the traffic could be received from other sources, such log feeds in SIEM.</li> <li>• Integration with Kubernetes ingress - Ammune integrates with ingress (reverse proxy based) instead of standard reverse proxy.</li> <li>• Inline integration - Ammune integrates in front of customers applicative architecture or between two hops in the flow.</li> </ul>

<b>Adhere to the 6 principles of energy literacy</b>	<p>This tool helps with all the 6 principles of energy literacy:</p> <ul style="list-style-type: none"> <li>• P1 – Economic security – security tools are needed more than ever because of the needs of more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> <li>• P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>• P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> <li>• P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The interconnected grid needs to have security tools implemented from the design phase.</li> </ul>
--	--

### 3.1.5. SIA OF SIEM TOOL

**Table 6. Societal impact assessment of SIEM tool in the EnergyShield project**

Name of the tool	Security Information and Event Management (SIEM)
Leading partner	KT
Contributing partners	SIMAVI, SC, Foresetti for final document review
Tool type	<b>Learning &amp; sharing</b>
Tool description including	EnergyShield SIEM tool aims to combine the security information management (SIM) with the security event

<b>algorithms that have a societal impact</b>	<p>management (SEM), forming a single collaborative security management system.</p> <p>This system collects critical information from multiple sources and endpoints. These endpoints can be:</p> <ul style="list-style-type: none"> <li>• Servers</li> <li>• Virtual Machines</li> <li>• Personal computers (laptops, desktops)</li> </ul> <p>from the critical infrastructure that SIEM is assigned to monitor. In the current project, the infrastructure is going to be the EPES sector and the assets from the SCADA system that are connected to one of the aforementioned endpoints.</p> <p>SIEMs are widely used on a plethora of infrastructures, to detect any suspicious activity and inform the end-user of suspicious activities. In the EnergyShield project, SIEM is hosted on SIMAVI's VPN with the rest of the toolkit, and it will detect and monitor the infrastructure's endpoint activities. The endpoints, where the agent can be installed, are Servers, VMs, laptops or Desktops. These endpoints must be linked to other assets involved in SCADA System (e.g., RTU, PMU etc.).</p>
<b>Identified societal issues</b>	<p>SIEM has implemented the following rules and active responses to protect the EPES value chain:</p> <ul style="list-style-type: none"> <li>• Buffer overflow attack</li> <li>• Attacks followed by the addition of a user</li> <li>• Network scan from same source IP</li> <li>• Buffer overflow attempt.</li> <li>• The browser has received an illegal datagram from a remote computer</li> <li>• The value for the parameter to the browser service was illegal</li> <li>• The browser driver has discarded too many mailslot messages</li> <li>• SQL injection attempt.</li> <li>• Multiple SQL injection attempts from same from same source IP</li> <li>• Shellshock attack attempt</li> <li>• sendmail: Rejected by access list (55x: Requested action not taken).</li> <li>• Auditd: replay attack detected</li> </ul>

	<ul style="list-style-type: none"> <li>• Apache: Multiple Invalid URI requests from same source.</li> <li>• Apache: Client sent malformed Host header. Possible Code Red attack.</li> <li>• Connection to rshd from unprivileged port. Possible network scan.</li> <li>• Perdition: Multiple connection attempts from the same source.</li> <li>• sshd: brute force trying to get access to the system.</li> <li>• sshd: authentication failed.</li> <li>• Endpoint Denial of Service</li> <li>• Exploitation for Client Execution</li> <li>• Exploitation of Remote Services</li> <li>• Exploitation for Privilege Escalation</li> <li>• Create Account</li> <li>• Web Service</li> <li>• Network Service Scanning</li> <li>• Exploit Public-Facing Application</li> <li>• Process Injection</li> <li>• Email Collection</li> <li>• Exploitation for Credential Access</li> <li>• Modify Registry</li> </ul>
<b>Requirements implemented in the tool</b>	<p>The EPES sector is affected by cyber-attacks. A SIEM is considered as an essential solution to protect the EPES sector against a variety of threat scenarios. It can identify anomalies in the system (SCADA systems etc.). As a result, alarms can be raised when a deviation is detected. A SIEM can provide valuable information to the SOC Analyst, which can help to mitigate and manage detected attacks. More key points of the value of SIEM are:</p> <ul style="list-style-type: none"> <li>• Prevent a single security vulnerability from compromising the entire infrastructure</li> <li>• Better adaptation to dynamic environments with fullyhosted security monitoring</li> <li>• Monitor all layers of the environment: infrastructure, hosts, containers, and applications</li> <li>• Discover security issues continuously or in real-time</li> </ul>

	<ul style="list-style-type: none"> <li>• Monitor at least 100 endpoints of the infrastructure</li> <li>• Powerful and easy to use tool for SOC analysts to monitor and prevent threats to their organisation's IT infrastructure, and to assess security systems and measures for weaknesses and possible improvements</li> </ul>
<b>Risk mitigation methods implemented by the tool developer</b>	<p>The easy deployment and the scalability of EnergyShield's SIEM make it fast and flexible and allow the processing of big amounts of data and having the possibility of performing event correlation at different layers with more complex rules.</p> <p>The interconnectivity with the other security tools within the project through Kafka offers a more flexible and evolved solution in terms of interconnection for the EPES sector. Kafka provides a quick and easy solution for the exchange of information between different tools. The correlation of events of different formats coming from different sources makes it an innovative tool for the SCADA infrastructure. The output of this tool will help security administrators in the threat analysis. The alignment with external sources like MITRE ATT&amp;CK [MTR21] and VirusTotal provides the functionality to analyse threats rapidly and easily filter security signals based on key attributes such as severity level or any associated entity, such as an attacker's IP-address based on infrastructure needs. This makes it scalable and can handle single, multiple keywords and string queries.</p> <p>The interconnection with the Automated Forensic tool empowers this functionality by providing information for the security threat events detected by the EnergyShield SIEM tool. Also, the Encryption tool can allow the security analyst to anonymise and search data in the encrypted domain using state-of-the-art homomorphic encryption techniques. This tool can extract any type of security event data and can provide the necessary levels of access control for multiple parties to search based on policies.</p> <p>The concept of "least privileges" to the SCADA systems based on roles that EnergyShield's SIEM can provide, is an innovative defence strategy that helps to minimise the unnecessary connections that can compromise the system to cyber-attacks.</p> <p>Another significant aspect is the capability to flag threats and catch misconfigurations across systems, applications, network, and infrastructure against EPES assets in a timely manner that offers an advanced and fast solution to SOC Analyst. After implementing the above functionalities, the</p>

	<p>correlation of the information enhances the situational awareness. The situational awareness represents the trust level of each EPES asset in the sub-network.</p> <p>Also, the tool is GDPR and NIST compliant as mentioned in the previous section, by offering pre-built reports and rule templates to help organisations address industry compliance requirements. It is scalable and can handle single, multiple keywords and string queries.</p>
<b>Adhere to the 6 principles of energy literacy</b>	<p>This tool helps with all the 6 principles of energy literacy:</p> <ul style="list-style-type: none"> <li>• P1 – Economic security – security tools are needed more than ever because of the needs for more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> <li>• P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>• P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> <li>• P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The interconnected grid needs to have security tools implemented from the design phase.</li> </ul>

### 3.1.6. SIA OF ENERGYSHIELD TOOLKIT

**Table 7. Societal impact assessment of EnergyShield toolkit in the EnergyShield project**

Name of the tool	EnergyShield toolkit
Leading partner	SIMAVI
Contributing partners	All tool providers
Tool type	<b>Learning &amp; sharing</b>
Tool description including algorithms that have a societal impact	<p>The toolkit integrates all the tools via the common platform and presents the links with the other work packages.</p> <p>The common platform is implemented on a cloud environment hosted by SIMAVI, on a Linux machine that hosts two major groups of components:</p> <ul style="list-style-type: none"> <li>• Standalone components like Kafka, PostgreSQL;</li> <li>• Docker containers (Keycloak, and all the other specific modules and tools).</li> </ul> <p>EnergyShield Portal is the place where there is a single point of access to the toolkit. It displays the data available from individual components, considering that the components might be deployed in the same place as the portal (common framework) or they are deployed on pilot premises, from where information is offered via a secured line and according to the security policy implemented by a pilot. The Portal is enabled to take advantage of using the outputs of components running as services (SaaS – Software as a Service).</p> <p>There is no direct interaction between the common platform or the portal with the environment where the Operational System is working.</p> <p>There are communication links between the technical components of the toolkit deployed on premises, and the common framework and the portal.</p> <p>The portal is also the place where the results of the event fusion system are run and where the results are presented.</p> <p>The event fusion mechanism is the central added value for the integrated toolkit, as it offers a global view of the <i>system as a whole</i>.</p> <p>Access to the portal is based on the user roles defined in the system. Only authenticated users have access, and the access is strictly monitored and is based on the security policy defined in each site (pilot site).</p>

<b>Identified societal issues</b>	<p>The EnergyShield portal will help secure the EPES value chain by offering an integrated view of the overall security posture by integrating in a graphical interface all the tools presented above.</p> <p>In order to improve the information shown to the user we have implemented the following advanced tools and concepts:</p> <ul style="list-style-type: none"> <li>- Event fusion - Data fusion is the process of incorporating different knowledge about an object to obtain a more detailed description [DIN17]. The goal is to include information about that object from multiple sources and thus obtaining synergy [MIT12]. Synergy is obtained when an object described has more information than the sum of its parts. Data fusion will gain [BEL02]: <ul style="list-style-type: none"> <li>○ Representation: fused data will have better abstract or granularity than data presented separately.</li> <li>○ Certainty: considering <math>U</math> a set of data and <math>P(U)</math> the data probability before fusion, then <math>P(U') &gt; P(U)</math>.</li> <li>○ Accuracy: data has less errors and noise than the data represented separately.</li> <li>○ Completeness: fused data is complete and less redundant.</li> <li>○ There are many fusion techniques, but for the project we'll use feature level fusion and decision level fusion.</li> </ul> </li> <li>- Continuous improvement by machine learning - The score based fusion mechanism is used to compute threat risks for the whole system. The risks are expressed as marks between 0 and 10, 0 means no risk, 10 means maximum risk. The initial application of the mechanism will use a supervised training mechanism based on existing data and simulated data. In the following stages, the feedback received from the operators of the SIEM tool will be used to retrain the system and get better results. The algorithms and the mechanism used are fully described in deliverable D1.5 System architecture [ESH21a]).</li> </ul>
<b>Requirements implemented in the tool</b>	<p>The common software platform presented below has five different deployment areas:</p> <ul style="list-style-type: none"> <li>● Assessment provides information on most critical attack vectors. It includes Vulnerability Assessment</li> </ul>

	<p>(VA) modules and Security Behaviour Analysis (SBA) tools.</p> <ul style="list-style-type: none"> <li>Monitoring and protection provide early warning on incoming attacks and malware. It includes Anomaly Detection modules and Distributed Denial of Service mitigation modules.</li> <li>Learning and sharing collects information from all the other modules and creates plans and instruction which refers to SIEM.</li> <li>Framework components are supporting components used by the whole deployment. They include container engine (Docker) Authentication and Authorization (Keycloak), Communication system (Kafka), REST, and Process management (Kubernetes ).</li> <li>Deployment system. It implements Continuous Integration/Continuous Deployment (CI/CD) mechanism. It is based on GitLab [GIT20]</li> <li>The platform is prepared to be placed in an OT environment with existing security mechanisms.</li> </ul>
<b>Risk mitigation methods implemented by the tool developer</b>	<p>The security of the EnergyShield portal is very important due to the sensitive data displayed. The sensitive data refers to EPES value chain system security. Security has played a very important role in the design of the EnergyShield portal by:</p> <ul style="list-style-type: none"> <li>We have implemented a graphical view of the security of the EnergyShield portal named System as a whole – this module depicts the toolkit security as a whole, depicted in images 53..57 from the deliverable D5.5 System release [ESH21b], that show the security of the system for each layer: component, communication, information, function, business.</li> <li>The deliverable D5.5 System release [ESH21b] presents in detail, in chapter 9, the security principles we have implemented (Chapter 9.1) and our SDLC process (Chapter 9.2).</li> </ul>
<b>Adhere to the 6 principles of energy literacy</b>	<p>This tool helps with all the 6 principles of energy literacy:</p> <ul style="list-style-type: none"> <li>P1 – Economic security – security tools are needed more than ever because of the needs for more energy consumption and grid connection to the internet and interconnection between IT and OT.</li> </ul>

	<ul style="list-style-type: none"> <li>• P2 – National security - The security of a nation is dependent on both the sources of energy it uses and the resilience of the grid. Grid resilience is very important, especially in case of cyber-attacks.</li> <li>• P3 – Environmental quality – the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P4 – Demand and quality of life - the use of clean energy increases the need for device interconnection and Internet access which translates in the need for better security tools.</li> <li>• P5 – Access &amp; quality of life - Energy is related to all walks of life: we need energy to use: air conditioner, running water, sewer system, internet, hospitals etc. A small disruption in the energy grid can have disastrous consequences in all parts of society. Thus, security tools need to be implemented in grid design.</li> <li>• P6 – Impact of energy to populations – Poor marginalised people can have access to energy by using simple solar panels to create their energy. The interconnected grid needs to have security tools implemented from the design phase.</li> </ul>
--	--

### 3.2. CROSS -EVALUATION OF TOOLS

In this section the factors that have the potential to determine a societal impact are mapped onto the specific EnergyShield tools in Table 8. Whether those risks will materialize depends on multiple factors including, but not limited to, the design and deployment choices.

**Table 8. Societal impact factors analysis**

	VA	SBA	AD	DDoSM	SIEM	Toolkit
<b>R&amp;I</b>						
Health and wellbeing		x		x	x	x
Food security						
Sustainable energy						
Green, integrated mobility						

Climate action						
Secure societies		x			x	x
Inclusive and reflective societies		x				
<b>Energy literacy</b>						
Economic security	x	x	x	x	x	x
National security	x	x	x	x	x	x
Environmental quality	x	x	x	x	x	x
Demand and quality of life	x	x	x	x	x	x
Access & quality of life	x	x	x	x	x	x
Impact of energy to populations	x	x	x	x	x	x
<b>Cyber- factors</b>						
Use of technology	x	x	x	x	x	x
Bulk monitoring and data collection	x	x	x	x	x	x
Data analysis (open data sources)	x	x	x	x		
Abnormal or deviant behaviour of forecasting tools (ML, AI)	x		x	x		x

Based on the issues raised by technology providers and the assessment performed some recommendations to limit the societal impact have arisen.

- Multi-tenant Software as a Service (SaaS) tools

Due to the stringent security requirements of critical infrastructure operators that have a high preference from on premise deployment on a security environment without internet access, we recommend deploying the product as a multi-tenant Software as a Service (SaaS) tool. (VA tool)

- Anonymization at its best

Companies need a tool for an independent assessment of the skills gaps in the organisation and to be able to also provide proper and equal access to cybersecurity awareness training to employees (SBA tool).

- Agnostic wave

OT industrial system need constant monitoring for work safety and electrical grid safety. Agnostic technologies put forward the monitoring technologies with limited human interaction. AD tool brings visibility into physical processes, to support intelligent, real-time action, enhanced by diagnosis and AI, empowering operators with timely alerts and actionable insights.

- Eyes on the attacks

Due to the multitude of attacks that occur real, a traffic enforcement module and analytics unit that provides near real time analytics of the traffic is required to stop these attacks.

- Constant supervision of system

The deployment of an overall SIEM due to its fast and flexible and feasibility to processing of big amounts of data and having the possibility of performing event correlation at different layers with more complex rules is recommended. The interconnectivity with the other security tools within the project through Kafka offers a more flexible and evolved solution in terms of interconnection for the EPES sector

- Least privileges to the SCADA

The concept of “least privileges” to the SCADA systems based on roles that EnergyShield’s SIEM can provide, is an innovative defence strategy that helps to minimise the unnecessary connections that can compromise the system to cyber-attacks. Additionally, the tool is GDPR and NIST compliant as mentioned in the previous section, by offering pre-built reports and rule templates to help organisations address industry compliance requirements. It is scalable and can handle single, multiple keywords and string queries.

- Flexibility is key

Starting from a plethora of technologies and use case functionalities, the EnergyShield system needs to provide full flexibility. In adapting and integrating technologies the technology providers have improved and adapted the tools making them ready for integration through the overall EnergyShield system and interacted with Practitioners to collect feedback (testing and evaluation of tools. Furthermore, a flexible integration concept was designed and is being implemented to ease the accommodation of tools and a Portal to securely access the toolkit. Technology providers have collaborated towards preparing and accommodating tools using different technologies in a common environment (EnergyShield toolkit) and using a data fusion mechanism combined with machine learning to create a global view.

## 4. CONCLUSION

This deliverable presents the societal impact that the EnergyShield project has. This document details how the tools can help society by security one of the most relied on critical infrastructures: the energy grid.

As online threats and cyber-attacks continue to permeate the Internet, it is essential that we as a community develop a better understanding of these issues and how they can impact our lives. For instance, in deliverable D8.3 we listed many published cyber incidents from the energy sectors of the last years.

Starting from H2020 societal challenges, adding the energy literacy principles and societal impact of cyber-attacks the EnergyShield tools and toolkit were assessed.

A set of recommendations to address the societal impacts and to limit the effects on the potential users of EnergyShield tools and toolkit were listed.

Awareness and domain literacy are among the most important aspects when dealing with new technologies and methods.

It is worth mentioning that the real societal impact of the results of EnergyShield project will be visible in the next years as the dedicated and adapted tools together with the toolkit used as a separate system will be implemented on the premises of different actors as part of the EPES value chain.

## 5. REFERENCES

- [BAB19] Babuta, Alexander, and Mation Oswald, “Data Analytics and Algorithmic Bias in Policing”, RUSI, 2019, p.7.
- [BEL02] D. Bellot, A. Boyer, and F. Charpillat, “A new definition of qualified gain in a data fusion process: application to telemedicine,” in Proceedings of the Fifth International Conference on Information Fusion, 2002, vol. 2, Jul 2002, pp. 865– 872 vol.2.
- [CEN12] CEN-CENELEC-ETSI Smart Grid Coordination Group Smart Grid Reference Architecture  
[https://ec.europa.eu/energy/sites/ener/files/documents/xpert\\_group1\\_reference\\_architecture.pdf](https://ec.europa.eu/energy/sites/ener/files/documents/xpert_group1_reference_architecture.pdf)
- [CLE22] Cleannet.org, “Energy and society”, Available Online: <https://cleannet.org/clean/literacy/energy7.html>, Last Access: 2022-04-12
- [COE17] Council of Europe, “Mass Surveillance”, 2017. Available at: <https://rm.coe.int/factsheet-on-mass-surveillance-final-rev1august2017/1680735d82>
- [DIN17] L. M. Dinca, G.P. Hancke, "The Fall of One, the Rise of Many: A Survey," IEEEAccess, no. Digital Object Identifier 10.1109/ACCESS.2017.2694050, 2017.
- [ESH16] EnergyShield Consortium (2022), D1.6 Data privacy and ethical compliance report
- [ESH21a] EnergyShield Consortium (2021) D1.5 System Architecture - final update
- [ESH21b] EnergyShield Consortium (2021) D5.5 System Release
- [EUA19] EU Agency on Fundamental Rights, Data quality and artificial intelligence – mitigating bias and error to protect fundamental rights, FRA, 2019. Available at: [https://fra.europa.eu/sites/default/files/fra\\_uploads/fra-2019-data-quality-and-ai\\_en.pdf](https://fra.europa.eu/sites/default/files/fra_uploads/fra-2019-data-quality-and-ai_en.pdf)
- [FUS19] Fussey, Pete, and Daragh Murray, “Bulk Surveillance in the Digital Age: Rethinking the Human Rights Law Approach to Bulk Monitoring of Communications Data”, Israel Law Review, Vol.52, Issue 1, March 2019, pp.31-60.
- [KRU95] Philippe Kruchten (1995). Architectural Blueprints—The “4+1” View Model of Software Architecture. Paper published in IEEE Software 12 (6) November 1995, pp. 42-50
- [LIK13] Li, Kan, Lin Zhang, and Heyan Huang, “Social Influence Analysis: Models, Methods, and Evaluation”, Engineering, Vol.4, Issue 1, Fall 2018, pp.40-46.

- [MAY13] Mayer-Schonberger, Viktor, and Lenneth Cukier, *Big Data: A Revolution that will transform how we live, work and think*, Hachette, London, 2013.
- [MIT12] H. B. Mitchell, *Data Fusion: Concepts and Ideas*. Berlin, Heidelberg: Springer Berlin Heidelberg, 2012. [Online]. Available: <http://link.springer.com/10.1007/978-3-642-27222-6>
- [MTR21] <https://attack.mitre.org/>
- [NUR18] Nurse, J. R. C. (2018). *Cybercrime and You: How Criminals Attack and the Human Factors that They Seek to Exploit*. In Attrill-Smith, A., Fullwood, C. Keep, M. & Kuss, D.J. (Eds.), *Oxford Handbook of Cyberpsychology* 2nd Edition. Oxford: OUP. <https://doi.org/10.1093/oxfordhb/9780198812746.013.35>
- [ONE16] O'Neil, Cathy, *Weapons of Math Destruction: How big data increases inequality and threatens democracy*, St Ives, Allen Lane, 2016.
- [PAS16] Report of the Protection and Security Advisory Group (PASAG) (2016) *Horizon 2020 - Societal Challenge 7: Secure societies – protecting freedom and security of Europe and its citizens*. [https://ec.europa.eu/home-affairs/system/files/2020-09/report\\_of\\_the\\_h2020\\_protection\\_and\\_security\\_advisory\\_group\\_-\\_pasag\\_en.pdf](https://ec.europa.eu/home-affairs/system/files/2020-09/report_of_the_h2020_protection_and_security_advisory_group_-_pasag_en.pdf)
- [SCH15] Schlehahn, Eva, Patrick Aichroth, Sebastian Mann, Rudolf Schreiner, Ifan Shepherd, and B.L. William Wong, “Benefits and Pitfalls of Predictive Policing”, 2015 European Intelligence and Security Informatics Conference (EISIC), September 2015. Available at: [https://www.researchgate.net/publication/304293638\\_Benefits\\_and\\_Pitfalls\\_of\\_Predictive\\_Policing](https://www.researchgate.net/publication/304293638_Benefits_and_Pitfalls_of_Predictive_Policing)
- [SOL06] Solove, Daniel J., “A Taxonomy of Privacy”, *University of Pennsylvania Law Review*, Vol.154, No.3, January 2006, pp. 477-560, p.487.
- [SUT12] Sutherland, Alan A., Lorraine Johnstone, Kate M. Davidson, Stephen D. Hart, David J. Cooke, P. Randall Kropp, Caroline Logan, Christine Michie, and Ruth Stocks”*Sexual Violence Risk Assessment: An Investigation of the Interrater Reliability of Professional Judgments Made Using the Risk for Sexual Violence Protocol*”, *International Journal of Forensic Mental Health*, Vol. 11, No. 2, 2012, pp.119-130, p. 120. .
- [WRI09] International Conference of Data Protection and Privacy Commissioners, *International Standards on the Protection of Personal Data and Privacy*, 2009, Article 22. Available at: [http://www.privacyconference2011.org/htmls/adoptedResolutions/2009\\_Madrid/2009\\_M1.pdf](http://www.privacyconference2011.org/htmls/adoptedResolutions/2009_Madrid/2009_M1.pdf)

- [WRI12]** Wright, David, "The state of the art in privacy impact assessment", *Computer Law & Security Review*, Vol.28, 2012, pp.54-61.
- [WRI13]** Wright, David, and Michael Friedewald, "Integrating privacy and ethical impact assessments", *Science and Public Policy*, Vol.40, 2013, pp.755-766.
- [WRI15a]** Wright, David, "Ethical Impact Assessment", in J. Britt Holbrook and Carl Mitcham (eds.), *Ethics, Science, Technology and Engineering: A Global Resource*, 2nd edition, Macmillan Reference, Farmington Hills, MI, USA, 2015.
- [WRI15b]** Wright, David, Michael Friedewald, and Raphaël M. Gellert, "Developing and testing a surveillance impact assessment methodology", *International Data Privacy Law*, Vol.5, Issue 1, 2015, pp. 40-53.
- [WRI15c]** Wadhwa, Kush, David Barnard-Wills, and David Wright, "The state of the art in societal impact assessment for security research", *Science and Public Policy* Vol. 42, Issue 3, 2015, pp.339-354.

## DEVELOPING THE CYBER-TOOLKIT THAT PROTECTS YOUR ENERGY GRID



[www.energy-shield.eu](http://www.energy-shield.eu)

