Innovation Actions

Critical Infrastructure Protection: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

Project: H2020–CIP-01-2016–740898

Critical Energy Infrastructure Security Roadmap

DEFENDER

Defending the European Energy Infrastructures

November 2018

Defending the European Energy Infrastructures

Project: H2020–CIP-01-2016–740898

Critical Energy Infrastructures Security Roadmap

Abstract: Effective and reliable operation of Energy Infrastructure is critical to the security, wellbeing and prospect of European Citizens. Highly reliable and flexible Critical Energy Infrastructure (CEI) depends on the ability of energy delivery systems to provide timely, accurate information to system operators and automated control over a large, dispersed network of assets and components.

This vast and distributed control requires communication among millions of nodes and devices across multiple domains, exposing energy systems and other dependent infrastructures to potential harm from accidental and malevolent cyber and physical attacks**.** CEIS-SG is a pan-European Group of experts created by the H2020 DEFENDER project to share information on CEI risks, incidents, threats and countermeasures, exchange reliability best practices.

This report is an initial version of the DEFENDER CEIS-SG roadmap towards a more secure and reliable CEI. The propose is to facilitate discussions and ideas that will shape the final version of the document.

Disclaimer

This document may contain material that is copyright of certain DEFENDER beneficiaries, and may not be reproduced or copied without permission. All DEFENDER consortium partners have agreed to the full publication of this document. The commercial use of any information contained in this document may require a license from the proprietor of that information.

The DEFENDER Consortium is the following:

Participant number	Participant organisation name	Short name	Country
01	Engineering Ingegneria Informatica SPA	ENG	Italy
02	THALES Research & Technology	THALES	France
03	SingularLogic S.A.	SiLO	Greece
04	SIEMENS SRL	SIEM	Romania
05	ENGIE S.A. (Energy Generation)	ENGIE	France
06	Studio Tecnico BFP SRL (Wind Farms/SME)	BFP	Italy
07	Electricity Transmission Operator (TSO)	ELES	Slovenia
08	ASM Terni SpA (DSO)	ASM	Italy
09	Ministero dell' Interno (Polizia di Strato)	PdS	Italy
10	Dr. Frucht Systems Ltd	DFSL	Israel
11	Venaka Media Limited	VML	UK
12	Power-Ops Limited	POPs	UK
13	e-Lex	ELEX	Italy
14	Institute for Corporate Security Studies	ICS	Slovenia
15	Rheinisch-Westfälische Technische Hochschule Aachen	RWTH	Germany
16	TEI of Sterea Ellada/Electrical Engineering Dept.	TEISTE	Greece
17	Uninova	UNI	Portugal
18	Jožef Stefan Institute	JSI	Slovenia

The information in this document is provided “as is” and no guarantee or warranty is given that the information is fit for any particular purpose. The user thereof uses the information at its sole risk and liability.

Important Notice: *The propose of the report is to facilitate discussions and ideas that will shape the final version of the document. It covers ideas and opinions of the individual authors and in many cases they should be considered as work in progress and may change at anytime*.

Document Revision History

Date	Issue	Author/Editor/Contributor	Summary of main changes
19.09.18	0.1	ENG	First version, ToC
16.10.18	0.2	ENG	Updated version
29.10.18	0.3	ICS	CEIS-SG Activities
14.11.18	0.4	TEISTE	Update of the roadmap
26.11.18	0.5	BFP	Internal Peer Review
29.11.18	0.6	ENG	Updates and corrections after BFP peer-review
30.11.18	1.0	TEISTE	Final Version

Table of Contents

List of Abbreviations

5G	Fifth Generation (mobile communications)
CEI	Critical Energy Infrastructure
CEIS-SG	Critical Energy Infrastructure Security Stakeholders Group
CERT	Cyber Emergency Response Team
CIP	Critical Infrastructure Protection
CSIR	Computer Security Incident Response Team
DES	Distributed Electricity Storage
DS-SLA	Dynamic Security Service Level Agreement
EE-ISAC	Energy-tailored Information Sharing and Analysis Centre
ECSO	European Cyber Security Organisation
ENISA	European Union Agency for Network and Information Security
E-SMIS	European Security Monitoring & Information System
EV	Electrical Vehicles
I2SP	Incidents Information Sharing Platform
IP	Internet Protocol
ISAC	Information Sharing and Analysis Centre
IT	Information Technology
LEA	Law Enforcement Agency
LPT	Large Power Transformer
NIS	Network and Information Security
PMU	Phasor Measurement Units
PPP	Public Private Partnership
PUF	Physical Unclonable Functions
RES	Renewable Energy Sources
SCADA	Supervisory Control And Data Acquisition
URLLC	Ultra Reliable and Low Latency Communications
SGSG	Smart Grid Stakeholder Group

1 Introduction

Modern critical infrastructures are increasingly turning into distributed, complex Cyber-Physical systems that need proactive protection and fast restoration to mitigate physical or cyber incidents or attacks. Most importantly critical infrastructure need protection from **combined cyber-physical attacks**, which are much more challenging, and it is expected to become the most intrusive attacks in the near future**.**

The **Critical Energy Infrastructure (CEI)** is considered among the most complex Cyber-Physical systems. Effective and reliable operation of Energy Infrastructure is critical to the security, wellbeing and prospect of European Citizens. European life as we know it is made possible by a vast network of processes that produce, transfer, and distribute energy as well as the interconnected electronic components, communication devices, and people that monitor and control those processes. Highly reliable and flexible CEI depends on the ability of energy delivery systems to provide timely, accurate information to system operators and automated control over a large, dispersed network of assets and components. This vast and distributed control requires communication among millions of nodes and devices across multiple domains, exposing energy systems and other dependent infrastructures to potential harm from accidental and malevolent cyber and physical attacks.

Cyber-physical threats to CEI can impact national and European security, public safety, and the national economy. CEI security is directly linked with huge (cascading) effects to other Critical Infrastructures, such as Water Supply, Telecommunication, Transportation, Industry, Finance and so on. As a result, CEI has already experienced complex cyber-physical attacks. Only in 2014, some 250 energy companies in the western Europe and the US were infected by Dragonfly 2.0 [1] and a virus called “Energetic Bear” [2], similar to Stuxnet [3]. At national level, the Ukraine power grid was cyber-attacked on December 2015 [4] and on January 2017 [5] [6], creating power outage and significant problems. Taking into account the importance of energy in our life and its influence on other Critical Infrastructures, CEI requests significant attention.

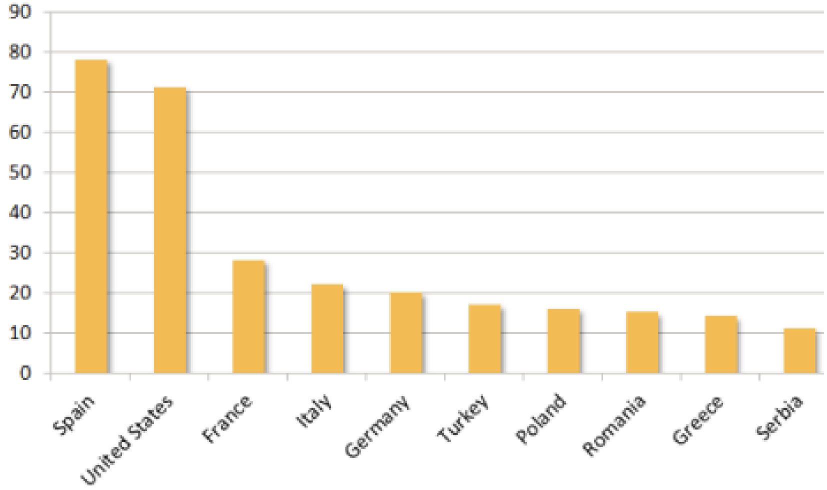


Figure 1: Dragonfly CEI attacks since 2014 [3]

To defend the CEI against combined cyber-physical threats, it is important to have an adequate understanding of the threat landscape, especially due to the fact that the consequences of an attack on any Critical Infrastructure would be dangerous and devasting. Greater awareness will lead to further protections in the future, while guidelines and standards would provide benchmarks to strive for to prevent cyber incidents. Compliance with standards can be one way of ensuring business continuity and can also be a tangible sign to trust for reliable service [7]. Defence against cyber-physical attacks may be based on tools to manage threats related to IT, such as ISO 27001 [8]. Since ISO 27001 has become an international standard for operators of Critical Infrastructure Information Security, many companies have implemented an Information Security Management System. SCADA systems, IT, Metering and

SAP Systems are single solutions without interconnection. However, considering CEI more complex and spatially-spread threats, it is most likely, that many operators are not able to detect or to react.

This document aims to define a widely agreed roadmap towards defending cyber-physical Critical Infrastructures in general, putting emphasis on CEI. The members of the DEFENDER consortium, with the collaboration and support from the CEIS-SG working group, contributed their expertise, ideas, and energy into this guiding framework. However, they strongly encourage every utility stakeholder owner, operator, researcher, vendor and policy maker to join forces and underpin the vision of a safer world. A common vision and a framework for achieving that vision are needed to guide the public-private partnerships that will secure energy delivery systems.

1.1 CEI Security Stakeholders Group

Aiming to enhance EU cybersecurity across critical sectors (i.e. energy, transport, water), the European Commission proposed the EU Network and Information Security directive (***NIS Directive),*** EU 2016/1148) [9] as part of the EU Cybersecurity strategy [10]. The NIS Directive aims to ensure that each Member State is equipped with a Computer Security Incident Response Team (CSIRT) and a national NIS authority, while the ENISA supported ***NIS cooperation group*** of CSIRTs and Cyber Emergency Response Teams (CERTs) aim to contribute towards information, threats and best practices exchange. CERTs have specialized knowhow in cyber threats anticipated prediction by leveraging on IT network traffic analysis, however they are very rarely specialized on energy sector. In parallel, a number of ***Information Sharing and Analysis Centres (ISAC)*** initiatives have been set up. ISACs can be tailored to the energy sector (forming Energy-tailored ISAC, EE-ISAC), aimed at facilitating information sharing on cyber-incidents among CEI stakeholders [11]. However, ISACs may lack on incident management capability. To exacerbate this situation, power operators have to respond to national and European electricity regulation agencies (NRAs, ACER, CEER, ENTSOE, EDSO), which have incorporated within their mandates some prescriptions and obligations for CEI stakeholder with respect to cyber-security management.

A variety of governance models, ranging from hierarchical, geographical-based, stakeholder-based, might be deployed to coordinate and synchronize the interaction and the information sharing among the utilities, CERTSs and ISACs, however so far, no specific obligation has been included in the NIS directive or in other regulation for adopting a specific governance model. As a result, smooth collaboration among CERTs, ISACs and CEI stakeholders has not yet been fully established, as currently utilities follow different, specialized, procedures and regulations. As such, **establishing combined cyber-physical CEI protection and pan-European collaboration and communication between CERTs, Utilities ISAC, EE-ISAC and European Electricity regulation agencies is fundamental**.

DEFENDER consortium assessed the above need for an *expert group* focused on the topic of CEI security, providing the opportunity for experts to address important issues in order to enhance CEI security in the EU. In that view, DEFENDER has initiated the **CEI Security Stakeholders Group (CEIS-SG)** to share information on CEI risks, incidents, threats and countermeasures, exchange reliability best practices, periodically review and challenge risk management practices to confirm that established security controls remain in place and changes in the energy delivery system or emerging threats do not diminish their effectiveness. Particular emphasis will be put on communicating stakeholder requirements so that CEI security studies and the achieved results can be further developed. Indicatively:

- Exchange and discuss about threats, vulnerabilities and incidents, to ensure that there is a common understanding affecting Critical Infrastructures, across the EU
- Give feedback on experiences with regulation and supervision to ensure effectiveness and efficiency
- Point to gaps and issues that require attention to ensure that important issues are being addressed
- Identify needs of stakeholders in the area of CEI security
- Identify channels to facilitate information collection, sharing and dissemination

- Identify additional elements that might be part of the CEI security.

Moreover, the CEIS-SG ecosystem promotes:

1. Engaged and information sharing at pan-European level on threats and best practices;
2. Risk-informed decision-making and the tools to facilitate it;
3. Adaptive learning, in which experiences serve as opportunities to inform and adjust future actions;
4. CEI security preparedness planning.

Members of the CEIS-SG Group have been selected based on excellence in the following skills: experience with information collection, sharing and dissemination; good understanding of policy and regulatory issues related to the security of CEI at national and/or pan European level including activities related to Critical Infrastructure Protection (CIP); knowledge of CIP and cyber security strategy and policy at national and/or pan European level; experience from interaction with relevant stakeholders/users. Experience with tools regarding all above knowledge of European policies on cyber security, as well as the specific requirements of the European CEI security is desirable for potential group members. The working language is English.

The founding members of the CEIS-SG, including internal and external members, are:

Name	Position	Affiliation
Dr. Massimo Bertoncini	H2020 DEFENDER Project Coordinator	Engineering-Ingegneria Informatica SPA
Dr. Gabriele Giunta	Research Specialist	Engineering-Ingegneria Informatica SPA
Prof. Theodore Zahariadis	H2020 DEFENDER Project Technical Manager	Head of Electrical Engineering Department, Technical Education Institute of Sterea Ellada
Dr. Paraskevi Kasse	Officer in Network and Information Security (NIS) Secure Infrastructures & Services Unit	European Union Agency for Network and Information Security (ENISA)
Dr. Mihai Paun	Vice-President Bruxelles	Centrul Român al Energiei (CRE)
Eng. Rui Pestana	System Operator Management Advisor	Rede Eléctrica Nacional, S.A. Portugal
Dr. Darko LUBI	Head of Government coordination group for CIP	Ministry of Defence Republic of Slovenia
Dr. Milan TARMAN	Special advisor to Director of National Security Authority (NSA) Republic of Slovenia	National Security Authority Republic of Slovenia
Ms. Simona Cavallini	Head of Research and Innovation Area	Fondazione FORMIT

1.2 CEI Security Roadmap – vision and scope

CEI Security Roadmap Vision: The European Union should protect legacy CEI and design a new generation of more resilient and self-healing European CEI able to survive large scale, combined, cyber-physical-social incidents and accidents, and guarantee the continuity of operations, while minimizing their cascading effects in the infrastructure.

Within the framework of a CEI Security Roadmap, the CEIS-SG and the DEFEDER Consortium will collaborate with many initiatives to address the evolving risks & threats in CEI, also providing feedback to other critical infrastructure authorities. The main goal is to support European CEIs to:

- **Survive:** Large scale, combined, cyber-physical-social incidents and accidents;
- **Guarantee:** Continuity of operations while minimizing the cascading effects;
- **Coordinate:** Safer CEI planning/roadmap.

CEI Security Roadmap Goal: The CEIS-SG, in collaboration with the DEFENDER Consortium, aims to assess and analyse physical, human and cyber threats and vulnerabilities of CEI and their cascading consequences to interrelated Critical Infrastructures and secure the efficient and resilient operation of existing and new CEI at pan-European through informed risk management, risk mitigation activities and countermeasures deployment, while accounting for the costs and benefits of security investments.

The CEI security roadmap strategies and priorities aim to inform and strengthen pan-European, government, industry, vendor, and academic programs designed to improve protection of energy delivery systems across the European Union.

In detail, the CEIS-SG Security roadmap scope may be summarized in the following:

- Define a framework that articulates the cyber-physical-human security needs of asset owners and operators in the energy sector. Focus is put on the Electricity sector, but it also directly applies to oil and gas sectors and indirectly to sectors such as water, transport and health.
- Provide high-level strategies for increasing the resilience of CEI, including legacy, state of the art and next-generation components, system, networks and procedures over the next 10 years.
- Guide industry, government, and research efforts to meet a common vision and create a permanent culture of security to sustain that vision.
- Encourage collaboration among all stakeholders to strengthen public-private partnerships and leverage expertise and capabilities across each stakeholder group.
- Encourage each stakeholder to plan and engage in efforts that directly align with one or more of the roadmap priorities.

1.3 CEIS-SG Manifest

Having a variety of profiles and expertise on topics related to CEI security, the CEIS-SG aims to play an important steering role in the development of this work and will contribute to DEFENDER yearly activities for the years to come. The basis of the CEIS-SG is documented in the **CEIS-SG Manifest** [12]. The Manifest has been the starting point for the CEIS-SG, showing an Energy Sector overview with a specific focus on the main CEI threat categories and Critical Infrastructures interdependences.

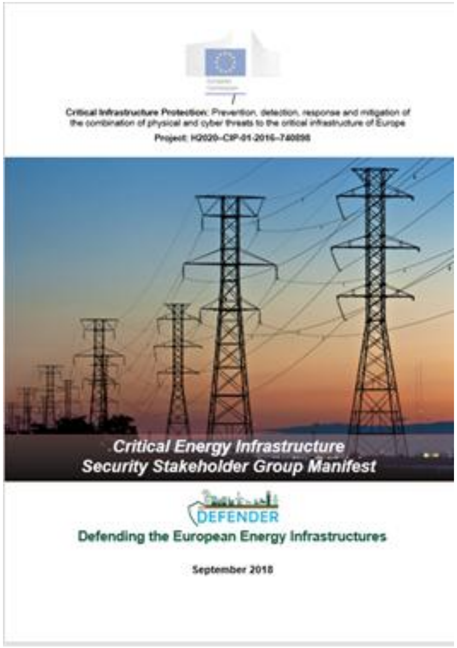
Despite the differences in what constitutes a CEI Security risk, several issues have been identified:

- Physical Security and Resilience
- Natural Disasters and Climate Resilience
- Aging Infrastructure and the risk of low Infrastructure investment
- Cyber security threats

- Growing gap in workforce development
- New unknown risks emerging from the combination of cyber and physical attacks and risk assessment

Another important aspect that is illustrated in the Manifest regards the interdependence aspect of CEI. The last couple of years, technical innovations and developments in digital information and telecommunications dramatically increased interdependencies among the critical infrastructures. The energy infrastructure provides essential fuel to all other critical infrastructure sectors, as without energy, none of them can operate properly. In turn, it depends on other critical infrastructure sectors, such as communications and information technology. A high-level overview of the interdependency among the critical infrastructures and the services that they offer and consume has been provided. Moreover, a CEI protection draft roadmap has been delivered in order to fix the next Group’s activities.

The **CEIS-SG Manifest** has recently been updated in October 2018 and approved by the CEIS-SG members. It has been published at the project web site http://defender-project.eu.



Critical Infrastructure Protection: Prevention, detection, response and mitigation of the combination of physical and cyber threats to the critical infrastructure of Europe

Project: H2020–CIP-01-2016–740898

Critical Energy Infrastructure Security Stakeholder Group Manifest

DEFENDER

Defending the European Energy Infrastructures

September 2018

Figure 2: CEIS-SG Manifest Cover page

2 Roadmap for CEI Security

The CEI is a landscape that has significantly changed the last couple of years. Smart technologies, including Smart Meters, Phasor Measurement Units (PMUs), Electrical Vehicles (EV) and Electrical Chargers, Renewable Energy Sources (RES) and Distributed Electricity Storage (DES) are introducing millions of new intelligent components to the energy infrastructure that communicate and control energy delivery in much more advanced ways than in the past. New infrastructure components and the increased use of mobile devices in energy infrastructure environments introduce new digital vulnerabilities and additional physical access points. New applications, such as managing energy consumption, involve new stakeholders (e.g., retail service providers, energy and financial market traders, industrial, commercial, and residential consumers) and require protection of private customer and energy market information. Because of the changing landscape, there is a need for a CEI security roadmap with broad focus on energy delivery systems, which include control systems, smart grid technologies, and the interface of cyber and physical security—where physical access to system components can impact cybersecurity.

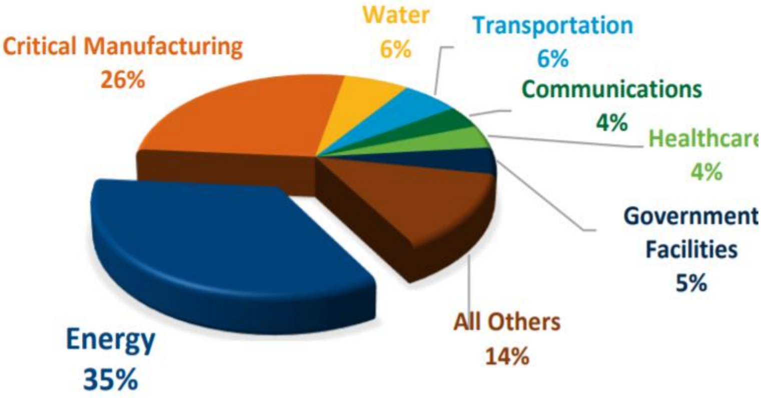


Figure 3: Incidents of Cyber Attacks in US in 2015

Beyond physical, more than ever before, CEI are vulnerable to cyber-attacks and cyber-threats. As reported by the US Department for Homeland Security, Industrial Control Systems Cyber Emergency Response Team (ICS-CERT) the energy sector experienced more cyber incidents than any sector from 2013 to 2015, accounting for 35% of the 796 reported incidents [13]. Taking into account the importance of energy in our life and its influence on other critical infrastructures, CEI requests significant attention. Adversaries have pursued progressively destructive means to exploit flaws in system components, telecommunication methods, and common operating systems found in modern energy delivery systems with the intent to infiltrate and sabotage them.

Last but not least, internal attacks or errors from the trusted **Humans-In-The-Loop (HITL)** due to e.g. lack of experience, insufficient training or lack of attention, are many times underestimated, though they form significant potential threats. Errors are at the heart of almost 17% of CEI breaches [14]. That included sharing confidential information or misconfiguring web servers. The clearest example of HITL error took place in November 2006, when lack of communication between the employees of two TSOs resulted in the largest European electricity blackout in the history.

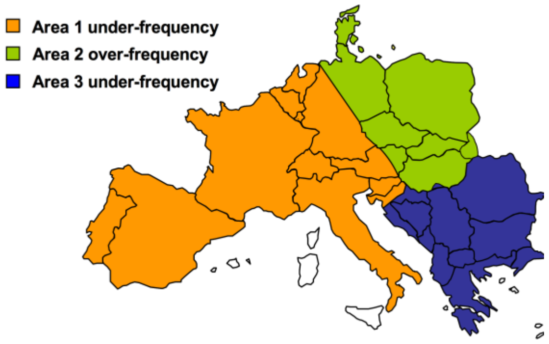


Figure 4: European blackout due to human error (Nov. 2006)

In general, it is agreed that it is not possible to completely protect the CEI [15]. While the bulk power system is designed with redundancy to manage planned equipment outages, and the resilience to withstand certain un-planned disruptions, it is not on a scale that would be sufficient to face the severe impact risks as the societal, environmental, and economic impacts would be sever. It would take decades to study, design, seek approvals, and build a security roadmap that would cover the complete CEI needs, while electricity customers would face enormous cost increases.

Yet, there are specific goals that a CEI security roadmap may have, which could be summarized in the following:

Target Goal 1: Enhance situational awareness of CEI stakeholders, utility owners and operators, industry, LEA, CERTs, CIRTs, policy makers and governmental organizations and researchers on the CEI requirements through robust, timely, reliable, and secure information exchange.

Target Goal 2: Contribute towards the definition of management principles and common agreed methodologies, procedures, metrics and labelling to enhance physical and cyber measures that improve preparedness, security, and resilience.

Target Goal 3: Initiate comprehensive emergency, disaster, and business continuity planning, along with training and large-scale exercises to enhance reliability and coordinated emergency response.

Target Goal 4: Enhance understanding of responsibilities and key interconnection, interdependency and collaborative roles with other critical infrastructure sectors to timely address risks and incidents.

Target Goal 5: Strengthen public and government regulatory activities and policies and contribute to the implementation of effective security, reliability and recovery efforts.

Current CEI security roadmap presents high-level strategies addressing the CEI security requirements, but it does not prescribe a single path forward. European and national policy makers, private organizations and PPP collaborations continue to produce unique cybersecurity solutions that meet the roadmap's defined needs and align with goals. Agencies and organizations, either independently or under the EU Network and Information Security (NIS) directive and ENISA coordination are encouraged to participate in cybersecurity efforts that will best capitalize on their distinct skills, capabilities, and resources while meeting their mission and needs. Contributions to relevant sectorial frameworks or regulatory initiatives will be achieved via the CEIS-SG ecosystem, which will sustain well after DEFENDER project as an autonomous stakeholders' group for shaping the CEI Security Roadmap.

2.1 New Threats and Vulnerabilities

The CEIS-SG has already identified various CEI security risks and threats, which have been categorized in the CEI Manifest. As a starting point, based mainly literature research [16], CEIS-SG and DEFENDER Consortium expertise, it's provided here a summary of requirements (Table 1) and trends (Table 2), which are affecting the European CEI secure operation:

Table 1: Current and evolving CEI Security Requirements

Current and evolving CEI Security Requirements
Timing Requirements
• Weeks for collecting long-term data, such as energy consumption information • Days for sharing information on long-term energy prediction • Hours for meter reading and planning energy pricing policy • Minutes for monitoring noncritical equipment and some market pricing information • Seconds for substation monitoring and feeder SCADA data • Sub-seconds for transmission wide-area situational awareness monitoring • ≤ 5 milliseconds for protective relaying
Integrity Requirements
• Data has not been modified without authorization • Source of data is authenticated • Timestamp associated with the data is known and authenticated • Quality of data is known and authenticated
Confidentiality Requirements

- Privacy of customer information
- Electric market information
- General corporate information, such as payroll, internal strategic planning, etc.

Table 2: Trends Affecting Future CEI cyber-physical-human Security

CEI physical security trends
Physical Security and Resilience risks
From physical view point, the CEI security will be affected by the increasing: • Terrorist attacks to the physical electric infrastructure such as Large Power Transformers (LPTs) and the infrastructure that control cyber components • Bombing, including arson and sabotage tactics. • Attacks from drones (including bombing) • Stealing the copper from the CEI network components, in many cases cutting off links and loops even under significant voltage. In this category, it's also include the aging Infrastructure and the risk of low Infrastructure investment
Natural Disasters and Climate Resilience risks
From natural disasters view point, the CEI security will be affected by the increasing: • Extreme and severe weather-related events, including lightning and storms • Natural disasters, such as floods, earthquakes, forest-fire and others, which may significantly impact the transmission and distribution network, and the reliability of electricity grids. • Cascading effects of extreme weather-related events and natural disasters, such as fallen trees on overhead lines.
CEI cyber security trends
Technology and Telecommunications risks
From technology and telecommunications view point, the CEI security will be affected by the increasing: • Systems interconnectivity and interoperability using IP-based communications • Convergence of information technology and telecommunications functions • Use of commercial off-the-shelf technologies • Reliance on wireless communications and 5G Ultra Reliable and Low Latency Communications (URLLC) features • Utilization of distributed intelligent devices and controls • Digital access points in energy delivery communication networks • Adoption of authentication and encryption techniques • Sophisticated detection and alarming mechanisms
CEI Cyber Operations risks

From CEI operations view point, the emerging and future CEI security will be affected by the increasing:

- Interconnection of business and control system networks
- Dynamic, market-based system control
- Need for real-time business and marketing information
- Utilization of distributed and alternative RES and DES
- Reliance on the telecommunications industry and the Internet for communications
- Reliance and availability of natural gas for electricity generation
- Interdependencies with other critical infrastructure (e.g., transportation systems and water)

CEI human security trends

Growing gap in workforce development risks

From human resources view point, the CEI security will be affected by the increasing:

- Aging workforce and staff turnover
- Loss of institutional knowledge, especially for professions such as lineworkers, which are heavily dependent on mentoring and on the job training.
- Need for new skills to address both operations and business information technology
- Use of corporate human resources for regulation compliance activities, which reduce the resources available for security enhancement

Third party risks

From third parties' cooperation view point, the CEI security will be affected by the increasing:

- Reliance on external providers for business solutions and services, which introduces additional cyber and physical reliability challenges
- Attention to consumer confidence and privacy concerns created by smarter Technologies
- Reliance on commercial off-the-shelf technologies

CEIS-SG has concluded that the ***main barriers in CEI security*** are summarized in the following table:

Table 3: Main barriers to CEI cyber-physical-human Security

CEI cyber-physical-human security barriers

- Threats are unpredictable and evolve faster than the ability to develop and deploy countermeasures
- Security upgrades to legacy systems are limited by investment and inherent technological limitations
- Testing of new control and communication solutions is difficult without disrupting operations
- Threat, vulnerability, incident and mitigation information sharing is not easy
- Weak business case for cybersecurity investment by industry
- Regulatory uncertainty in energy sector cybersecurity

2.2 Strategies for securing CEI

To offer efficient and effective CEI protection from cyber/physical/human events, we consider that four strategies should be implemented:

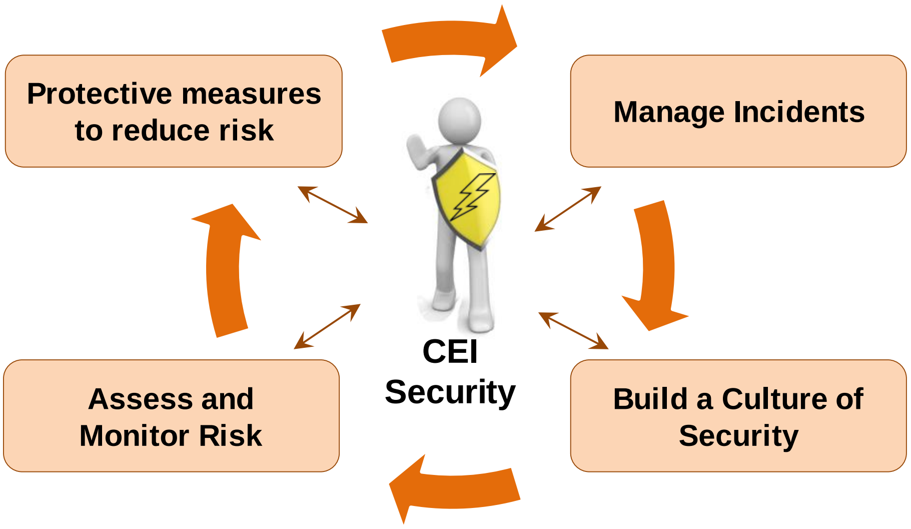

Protective measures to reduce risk
Manage Incidents
Assess and Monitor Risk
CEI Security
Build a Culture of Security

Figure 5: Securing CEI strategies

- **Assess & Monitor Risk.** This strategy gives to energy sector asset owners, utilities and service providers a thorough understanding of their current security posture, enabling them to continually assess evolving cyber/physical threats and vulnerabilities, their risks, and potential countermeasures. Implementing this strategy will help the stakeholders achieve continuous security state monitoring of all CEI and across cyber-physical domains.
- **Protective measures to reduce risk by design**. New protective (proactive) measures will be developed to reduce system risks (including vulnerabilities and emerging threats). These measures will be built into next-generation CEI and will help the electricity infrastructures stakeholders to offer CEI “defence in depth and by design” and offer components that are interoperable, extensible, and able to operate even in a degraded condition during a cyber incident.
- **Manage Incidents**. Managing incidents is critical, as physical disasters can be generalized, cyber assaults can be sophisticated and at the end any system can become vulnerable to emerging threats as absolute security is not possible. When protective measures are not applied or fail to prevent an incident, detection, remediation, recovery, and restoration activities should minimize its impact and quickly return to normal operations.
- **Build a Culture of Security.** Post-incident analysis and forensics enable CEI stakeholders to learn from the incident. Integrated with reliability practices, risk management practices will be periodically reviewed and challenged to confirm that established security controls remain in place, while physical and cyber-security best practices should be disseminated at pan-European level.

Through the roadmap development and implementation process, the CEIS-SG has defined a set of strategies, milestones and goals which are summarized in Table 4:

Table 4: Strategies and milestones for CEI security

Strategies			
1 Risk Assessment	**2. Protective Measures**	**3. Manage Incidents**	**4. Culture of Security**
Near-term Milestones (Project Duration)			
1.1 Common terms and measures specific to each CEI segment. 1.2 CEI segments categorization in Security Tiers	2.1 Evaluate the robustness and self-healing of new platforms, systems, networks, architectures, and policies	3.1 Tools to identify incidents across all levels of CEI 3.2 Tools to support and implement incidents management commercially available	4.1 Public awareness of CEI resilience efforts 4.2 Pan-European Stakeholders group to share mitigation strategies and define a security roadmap
Mid-term Milestones (4–7 years) By 2024			
1.3 Majority of infrastructure and asset owners baseline their security posture via energy subsector specific metrics	2.2 Scalable access control for all energy delivery system devices available 2.3 Next-generation, interoperable solutions for secure communications	3.3 Incident reporting guidelines accepted and implemented by each energy subsector 3.4 Real-time forensics capabilities and cyber event detection tools commercially available	4.3 Active Involvement of Humans in the Loop for CEI protection using trusted blockchains' based bidirectional information flows 4.4 Compelling business case developed for investment in CEI security
Long-term Milestones (8–10 years) By 2028			
1.4 Cyber-physical risk assessment tools commercially available	2.4 Self-configuring infrastructure enables operations' continuation during incidents	3.5 Lessons learned and best practices from cyber/physical incidents shared and implemented	4.5 Significant increase in the skilled employees and volunteers in CEI security
Goals			
Security monitoring of all CEI levels and across cyber-physical domains	**CEI architectures able to continue operating during cyber/physical incidents**	**Fast self-mitigation of cyber/ physical incidents, quickly return to normal operations**	**CEI security practices shared among stakeholders, academia, and government**

The CEIS-SG working group and the DEFENDER consortium are working on assessing the main activities and lines of action according to initial ideas and the above established strategies, namely Risk Assessment; Protective Measures; Manage Incidents; and Culture of Security, using a draft plan, which allows a more systematic assessment.

2.2.1 Risk Assessment

Risk Assessment Goal: Continuous security state monitoring and risk assessment of all CEI architecture levels and across cyber-physical domains is widely adopted by all CEI and energy asset stakeholders, owners and operators

Proper prevention and handling of incidents is possible only by providing risk assessment and effective situational awareness. However, defining common accepted organizational and normative processes for proper understanding of the risks and threats that affect the functioning of organizations is a challenging security task that needs appropriate technological support. Understanding the full depth and breadth of the security posture of CEI allows operators and stakeholders to determine and prioritize appropriate corrective actions quickly and effectively.

To gain deep understanding of CEI operation and risks, reliable and widely accepted security metrics are needed, as well as tools and methodologies for measuring and assessing both static and real-time security states to support risk management decision making. Because of the unique configurations of many CEI control systems, CEI operators need the tools to conduct self-assessments. The industry eventually needs security state monitoring tools that trigger autonomic, dynamic and evolving/adapting corrective and self-healing actions, while allowing the operators to override them, if necessary. The new threats that are detected and analysed would give added value to the existing analyses of the physical and cyber environments. Of course, the analysis is refining further impact assessment of threats to the smooth functioning of not only the electro-energy sector and all its domains, but also other sub-sectors of critical infrastructure, which due to their interdependence could be affected.

Special attention should also be paid on process standardization in the field of Risk Assessment. Currently in the DEFENDER project, appropriate opportunities for the further standardization of certain processes that bring some additional procedural and technological solutions of Risk Assessment have a fundamental role.

Table 5: Risk Assessment Milestones

Milestones
Near-term Milestones (Project Duration)
• Common terms and measures specific to each CEI segment. • CEI segments categorization in Security Tiers
Mid-term Milestones (4–7 years) By 2024
• Majority of infrastructure and asset owners baseline their security posture via energy subsector specific metrics
Long-term Milestones (8–10 years) By 2028
• Cyber-physical risk assessment tools commercially available

2.2.1.1 Main Barriers to Risk Assessment

The main barriers to risk assessment of CEI threats may be summarized in the following:

- *The energy sector faces rapidly changing threats that are difficult to predict or quantify.* Threats are changing over time. As such, understanding and properly categorizing the threat is a major challenge. Ambiguous and uncertain threats are difficult to be quantified. While advanced tools and methodologies to provide a deep analysis of attack vectors and resulting consequences are underway, commonly used risk analysis capabilities are still limited to the survey and analysis of critical assets.

- *Not consistency on criteria, methods and metrics to assess risk.* Many CEI and energy asset owners and operators are performing self-assessments of their control systems. However, the methods and metrics they use continue to vary. Risk factors (threat, vulnerability and consequence), consistent criteria, benchmarking and comparing energy delivery systems risk and evaluating the impact of security efforts is difficult. Moreover, baseline security of CEI is not consistent and widely accepted by all energy sector stakeholders.

Lack of processing and information exchange frameworks in pan-European level. In many cases, risks are not local but pan-European. Though, the NIS Directive aims to ensure that each Member State is equipped with a CSIRT and a national NIS authority, sharing of information and processing vast quantities of disparate data from a variety of sources (e.g., business, information, production, delivery, consumer, market, and other energy systems) and levels of granularity (e.g., sub-seconds to months) into actionable and timely knowledge that provides situational awareness of cybersecurity posture is a significant challenge.

- *Increasing complexity and interconnections* with telecommunications, RES, DES and smart grid networks introduce new vulnerabilities that can propagate across multiple domains.

2.2.1.2 Priorities to achieve milestones on Risk Assessment

To achieve the milestones on Risk Assessment, including real-time situational awareness, advanced technologies are needed that identify, acquire, correlate, analyse and visualize cyber and physical security-related data from all levels of the CEI ranging from component, device, system, asset and network and across the cyber-physical domains.

Table 6: Risk Assessment priorities roadmap

Priorities
Definition priorities
Key metrics to be defined include: • industry attack surface metrics released annually with industry agreed upon parameters • relative security posture before and after deployment of security solution • testing and baselining energy delivery systems security • labelling of delivery system cyber-physical risk levels according to current mitigation need • quantification of trustworthiness of a component, system, asset and “system of systems • characterization of threat scenarios and metrics for assessing energy delivery systems risk • security and results in terms of prevent, detect, and respond
Development priorities
There is an increasing need to develop: • methods to better identify and characterize threats • deceptive reasoning algorithm(s) to counter plausibility, assertions, and threat hypotheses • tool to assess and benchmark CEI risk, frameworks for prioritizing control measures, create risk-level matrix that balances threat, vulnerability, and consequence, and means for justifying costs • engineering decision making tools for optimizing security • distributed security state estimator that is tailored to multiple users and used by autonomous agents • tools to determine how and which vulnerabilities and threats should be addressed; track financial losses resulting from cyber incidents; and develop ability to trace vulnerabilities to financial losses • modelling and simulation tools that have dynamic automated capabilities to discover implication of complexities and inform risk management decisions • modelling, simulation and visualization tools for real-time security state monitoring of device management and control of new and legacy system applications, including visualization technologies that integrate and correlate multiple data streams

2.2.2 Protective measures

Protective measures Goal: Protective and by-design solutions should be defined to reduce the risk and enable CEI networks and systems to continue operating during cyber/physical incidents and attacks

Fast self-mitigation of cyber/ physical incidents, quickly return to normal operations

After risk assessment and attacks identification, well accepted protective measures should be applied to make legacy and next-generation CEI more resilient. The Protective measurements ultimate objective is to enable CEI to operate or at least implement critical functions during an incident or attack, and return to normal operations after the incident with minimal cascading effects to interconnected systems and infrastructures. As "protective measures" may be considered tools, procedures, methods and security architectures for fixing known attacks and ensure an integrated and balanced security approach spanning the entire life cycle of the CEI. The most comprehensive security improvements are realized "by-design" with the development and adoption of next-generation CEI architectures, self-configuring and self-adapting infrastructure and 5G communications that incorporate advanced interoperable components, which are inherently secure and offer enhanced functionality and performance.

Table 7: Protective Measures Milestones

Milestones
Near-term Milestones (Project Duration)
• Evaluate the robustness and self-healing of new platforms, systems, networks, architectures, and policies
Mid-term Milestones (4–7 years) By 2024
• Scalable access control for all energy delivery system devices available • Next-generation, interoperable solutions for secure communications
Long-term Milestones (8–10 years) By 2028
• Self-configuring infrastructure enables operations' continuation during incidents

The DEFENDER project brings a whole set of new technological solutions and measures in the field of physical and cyber security. These new technological solutions will bring additional quality to the area of proactive measures, which can be transferred to some extent into other organizational environments.

2.2.2.1 Main Barriers to Protective Measures

The main barriers to CEI Protective Measures may be summarized in the following:

- *CEI architectures are widely distributed and incredibly complex*. As a result, it is quite challenging to secure hundreds of substations and transformers, and millions of smart meters, RES and DES with limited processing and storage capabilities. In addition, CEI complexity increases exponentially with an increase in number of nodes, especially as smart meters are in many cases located in areas that are easily accessible and vulnerable to physical tampering or misuse.
- *Difficulty to provide quality data and robustness without introducing latency issues or introducing serious operational issues.* Traditional IT solutions and testing tools may disrupt, disable or shut down CEI because the operating performance requirements are very different
- *New "by-design" solutions are quite expensive.* In many cases, protective systems are not as fast as attack systems, while it is too difficult to deploy technologies that are both scalable and interoperable. Moreover, replacing CEI assets and implementing self-healing solutions by design (e.g. double virtualization) ensure reducing of the risk bit introduce a significant cost.

2.2.2.2 Priorities to achieve milestones on Protective Measures

To achieve the milestones on Protective Measures, resilient and robust architectures, attack-resistant platforms, secure field equipment, front-end processors, real-time operating systems, and other systems are needed. Technology advancements can include the development of hardened and tamper-safe field devices, such as programmable logic controllers, FPGAs and remote terminal units, or security appliances that can be installed with each critical asset/field device to protect it from malicious attack, offering another layer of defence. While CEI deployed across the electricity, oil and natural gas sectors have similar features, each application has unique characteristics that require fine-tuning and careful configuration. As such, secure communication architectures are needed within the context of each subsector, and they must be hardened against cyber/physical attacks and be able to continue operating in a degraded condition.

Secure remote access control is becoming increasingly important, including securely exchange of cryptographic keys using algorithms with minimal computational requirements, such as Physical Unclonable Functions (PUF) and involvement of secure 5G URLLC communication types.

Table 8: Protective Measures priorities roadmap

Priorities
Definition priorities
Resilience planning, instantiation, testing and validation design include: • Secure tiers labelling and guidelines for evaluating security robustness of next-generation CEI architecture, systems and networks; including architectures and guidelines for the capability • White list capabilities for applications and communications • Guidelines to manage changes in the configuration of CEI environments in a trusted way (e.g. use blockchains to ensure traceability) • New algorithms, based on PUF encryption for remote devices such as smart meters, to balance among security and computational complexity • Safe designs to prevent cascading failures • Techniques to provide explicit, managed communications trust • Security life cycle procurement specifications to guide vendor product development.
Development priorities
There is an increasing need to develop: • real-time adaptive security infrastructure that makes authorization and policy management an on-demand service for all systems and devices • tools to evaluate candidate architectures, concepts, and protocols before devices are built and tools for automated code review in both static and runtime environments • Software architectures that can isolate the impact of exploited internal/external vulnerabilities • Control systems that inherently defend themselves against internal and external threats • Solutions based on technologies such as the blockchains to provide built-in traceability and trust. • Advanced cryptographic key management methods for securing millions of devices, based on PUF encryption to balance among security and computational complexity • Communication methods, based on 5G security features and SCADA/EMS protocols to meet security and privacy requirements

2.2.3 Manage incidents

Manage incidents Goal: CEI should include several elements that are both proactive and reactive in nature to enable fast self-mitigation of cyber/ physical incidents and quickly return to normal operations

Managing CEI security cyber-physical incidents should include several proactive and reactive measures to ensure that the CEI is properly prepared to respond to an attack and can react effectively when an incident occurs, minimizing any side- or cascading-effects. Proactive measures include planning, incident prevention and post-incident analysis of lessons learned. Reactive measures include detecting and managing an incident or attacks as soon as it occurs.

Due to dislocated dispersion and complexity of the CEI, it is quite important to invest in the proactive measures, in order to simplify the reactive measures. Nevertheless, there is a clear need for tools to detect, identify, analyse and manage incidents including not only cyber-physical security but also associated forensics.

Table 9: Manage Incidents Milestones

Milestones
Near-term Milestones (Project Duration)
• Tools to identify incidents across all levels of CEI • Tools to support and implement incidents management commercially available
Mid-term Milestones (4–7 years) By 2024
• Incident reporting guidelines accepted and implemented by each energy subsector • Real-time forensics capabilities and cyber event detection tools commercially available
Long-term Milestones (8–10 years) By 2028
• Lessons learned and best practices from cyber/physical incidents shared and implemented

2.2.3.1 Main Barriers to Manage Incidents

The main barriers to Manage incidents and attacks to CEI may be summarized in the following:

- *Very strict time constraints*. CEI have very strict time constrains. In case of substation management and electricity rerouting the time interval to avoid blackouts is in many cases in the range of milliseconds. Existing tools need some time to detect and identify the incident or the attack and additional time to apply countermeasures. Especially if the complete process is not fully automated and the human factor is somehow involved.
- *Complex operation and reaction*. While automated methods of incident detection can be extremely valuable in preventing exploits to CEI, a proper balance of automation is essential for the application of countermeasures due to extreme CEI complexity and numerous side-effects that an action may have. Traditional IT solutions can disable or shut down energy delivery systems with side-effects to CEI operation and cascading effects to other critical infrastructures.
- *Unclear responsibilities' distribution*. The roles and responsibilities among stakeholders, CEI owners and operators are not always clear. A variety of governance models, ranging from hierarchical, geographical-based, stakeholder-based, might be deployed to coordinate and synchronize the interaction and the information sharing among the utilities, CERTSs and ISACs, however so far, no specific obligation has been included in the NIS directive or in other regulation for adopting a specific governance model. As a result, smooth collaboration among CERTs, ISACs and CEI stakeholders has not yet been fully established, as currently utilities follow different, specialized, procedures and regulations.

2.2.3.2 Priorities to achieve milestones on Manage Incidents

CEI are very complex critical infrastructures and automated actions may have severe side and cascading effects. Given the vast numbers of automation components in the smart grid and in many modern oil and natural gas infrastructures, providing actionable information will become more important in understanding the overall health of the CEI. Innovations in distributed decision making approaches will play a more prevalent role than hierarchical command-and-control approaches to ensure that the system behaves much like an ecosystem, in which some portions may be impacted by varying degrees, but the remainder of the system reacts to contain the damage and continue operating the critical functions until the incident has passed and the system is returned to normal service [16].

Real time tools are needed not only to assist in the detection of incidents, but also Artificial Intelligent based frameworks are required to advise on the needed mitigation/recovery actions.

Table 10: Manage Incidents priorities roadmap

Priorities
Definition priorities
Incident Mitigation/countermeasure actionable decisions' design include: • Capabilities to measure the degree of resilience, including the impacts of a cyber/physical incident • Adaptation of intrusion prevention system for more robust application to network and application • Identification of existing incident reporting guidelines, blueprints and best practices • Easy to follow approaches to incident reporting for the CEI sector and a common system/ interoperable systems for reporting incidents by critical infrastructure sector • Training material and procedures to evaluate cyber incident, including the probability of escalating to a national or pan-European scale incident and response.
Development priorities
There is an increasing need to develop: • real-time assisted and Artificial Intelligence/Machine Learning supported tools, focused on the detection, analysis and recovery/restoration actions in response to a cyber-physical incidents • specialized sensor systems (e.g. an increased number of low-cost PMUs) to overview the CEI operations quality, detect and report anomalous activity • technology to handle terrorist attacks, including attacks with drones • tools to simulate operational energy delivery systems' security incidents for training and incident handling purposes • audit trail capability for intrusion detection systems to enable automated reporting • communication tools, based on 5G security features and SCADA/EMS protocols to apply security and privacy countermeasures with low latency and high reliability

2.2.4 Culture of Security

Culture of Security Goal: Provide tools, platforms, procedures and means to share CEI security practices among stakeholders, industry, academia, government and policy makers

Creating external awareness and knowledge building within targeted industrial communities is one of the most important goals to protect legacy and future CEI. Humans in the Loop, either employees or LEA are vital to sustaining critical functions in large CEI, particularly in the face of system volatility or stress [17].

A culture of security promotes working in a secure manner, rewards sharing of security risk information, and encourages a sustained level of attentiveness at the individual, small group, and organizational levels, and across many organizations [16].

Extensive dialogue should be ongoing, by various means and with sufficient breadth and depth of reach to affect the attitudes and behaviours of citizens, policy makers, CEI and utility owners and operators, and stakeholders about the importance of CEI security and the consequences of operating under certain levels of risk. It is necessary to establish a system of raising the awareness of all subjects from employees, management of organizations in the energy field, state institutions directly or indirectly charged with the development of risk management legislation and standards, professional associations, international environment and, last but not least, an individual that is part of the environment where CEI operate.

Table 11: Culture of Security Milestones

Milestones
Near-term Milestones (Project Duration)
• Public awareness of CEI resilience efforts • Pan-European Stakeholders group to share mitigation strategies and define a security roadmap
Mid-term Milestones (4–7 years) By 2024
• Active Involvement of Humans in the Loop for CEI protection using trusted blockchains' based bidirectional information flows • Compelling business case developed for investment in CEI security
Long-term Milestones (8–10 years) By 2028
• Significant increase in the skilled employees and volunteers in CEI security

2.2.4.1 Main Barriers to Culture of Security

The main barriers to a Culture of Security to CEI may be summarized in the following:

- *Growing gap in workforce development*. CEI stakeholders, energy utilities and operators face a critical shortage of engineers and skilled craft workers. There is a lack of highly educated staff with broad skill sets (including IT skills) to manage future operations. New technologies are rapidly changing the CEI environment, so that experienced personnel is hard to be trained on the new automated systems. On the other hand, new employees do not have the time to be sufficiently trained by the experienced employees. As such there is limited knowledge and incomplete understanding of CEI security risks and cost of decisions and system resilience in terms of failure modes and vulnerabilities.
- *Security standard compliance is not always sufficient.* While standards have helped to raise security to a baseline level across the sector, some standards remain unclear or too broad, or may have prompted utilities to use less advanced security measures to meet requirements. In addition, a rapidly changing risk environment means standards compliance today may not be sufficient tomorrow.
- *Patching/fixing vulnerabilities in CEI is costly and may create new cyber risks.* The cost of fixing a software vulnerability discovered during acceptance testing is about 15 times greater than the cost of fixing it during the design phase [18]. Moreover, patching a newly integrated system takes time, to prove that it does not compromise normal CEI functionality prior to implementation.

2.2.4.2 Priorities to achieve milestones on Culture of Security

Building a culture of security requires increased executives' engagement to help government decision and policy makers better understand CEI security issues and to make resource investment decisions. In this direction CEI-SG is the DEFENDER seed towards a culture of security. Moreover, best practices in safe code development and integration can be promoted by the energy sector and universities. Vendors can employ best product development practices. Although these practices may not eliminate all software vulnerabilities, promoting a security culture has shown to make a difference in the products security levels.

Table 12: Manage Incidents priorities roadmap

Priorities
Panning priorities
Building a culture of security includes: • Establishing high-level meetings with governmental and policy makers, along with ENISA, members of the European Parliament and ad-hoc groups (e.g. European Cyber Security Organisation, ECSO) to gain support • Analysing of the incentives and benefits of implementing security beyond mandatory standards to help fortify the business case • Identifying and disseminating best practices for connecting secure and resilient CEI and communications networks (e.g., deploy firewalls, intrusion detection systems, antivirus solutions) • Identifying best practices for managing the risk at the cyber-physical interface of field equipment • Training material and procedures to evaluate cyber incident, including the probability of escalating to a national or pan-European scale incident and response. • Promoting the benefits of a career in cybersecurity for energy delivery systems
Development priorities
There is an increasing need to develop: • a roadmap to address legal aspects of collaboration, leveraging existing and forthcoming agreements • a roadmap outreach plan to increase awareness and garner support for roadmap implementation efforts • best practice periodicals that focus on techniques, practices, procedures, and polices for energy sector operators, engineers, and technical staff to encourage widespread adoption • a program to independently validate that components and systems conform to best practices • a voluntarily populated matrix of vendors and asset owners conducting vulnerability assessments and applying best practices • certification procedures and methodologies towards estimation of risk and CEI Tiers classification and DS-SLAs for electricity asset owners and develop a strategic implementation plan to gain widespread adoption • a certification program that shows results of vulnerability testing and secure coding practices • a trusted and traceable platform (e.g. based on blockchains) for information exchange between stakeholders and utility owners/operators on potential incidents and attacks

3 Future plans

The presented CEI security roadmap provides a summary of various discussions and exchange of ideas that have taken place within the CEIS-SG and the DEFENDER consortium meetings. A number of high-level strategies addressing the CEI security requirements are presented including main barriers and priorities.

It should be underlined that the propose of the report is to facilitate discussions and ideas that will shape the final version of the roadmap. The current version covers ideas and opinions of the individual authors and in many cases, they should be considered as "*work in progress*", not always agreed, and may change at any time.

CEI stakeholders as part of CEIS-SG or individually, utility owners and operators, energy and IT industries, agencies, LEAs, governmental and European organizations, either independently or under the EU NIS directive and ENISA coordination are highly encouraged to participate in the discussion while meeting their mission and needs.

4 References

[1] A. Greeberg, “Hackers gain Direct access to US power grid controls,” 09 06 2017. [Online]. Available: https://www.wired.com/story/hackers-gain-switch-flipping-access-to-us-power-systems/.

[2] G. Desarnaud, “Cyber Attacks and Energy Infrastructures,” January 2017. [Online]. Available: https://www.ifri.org/sites/default/files/atoms/files/desarnaud_cyber_attacks_energy_infrastructures_2017_2.pdf.

[3] “‘Dragonfly’ Malware Highlights Vulnerability of Energy Infrastructure,” [Online]. Available: https://www.triplepundit.com/2014/07/dragonfly-malware-highlights-vulnerability-energy-infrastructure/.

[4] “December 2015 Ukraine power grid cyberattack,” [Online]. Available: https://en.wikipedia.org/wiki/December_2015_Ukraine_power_grid_cyberattack.

[5] “Ukraine power cut 'was cyber-attack',” BBC News, [Online]. Available: https://www.bbc.co.uk/news/technology-38573074.

[6] “Ukraine's power outage was a cyber attack: Ukrenergo,” REUTERS, [Online]. Available: https://www.reuters.com/article/us-ukraine-cyber-attack-energy/ukraines-power-outage-was-a-cyber-attack-ukrenergo-idUSKBN1521BA.

[7] E. N. Hunter, A Comparative Analysis of Cybersecurity Guidelines and Standards for Nuclear Power Plants. Master Thesis ITC70LT, Tallinn University of Technology , 2016.

[8] A. J. Segovia., “The ISO 27001 & ISO 22301 Blog. “How can ISO 27001 and ISO 22301 help with critical infrastructure protection?”,” 2017. [Online]. Available: https://advisera.com/27001academy/blog/2017/09/25/how-can-iso-27001-and-iso-22301-help-with-critical-infrastructure-protection/.

[9] “DIRECTIVE (EU) 2016/1148 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL,” European Parliament, 06 June 2016. [Online]. Available: https://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016L1148&from=EN.

[10] “The EU Cybersecurity strategy,” [Online]. Available: http://europa.eu/rapid/press-release_IP-13-94_en.htm.

[11] ENISA, “Information Sharing and Analysis Centres (ISACs),” 2017.

[12] DEFENDER Consortium, D6.2 - CEI Security Stakeholder Group Manifest, 2017.

[13] U.S. Department of Energy, “Multiyear plan for Energy Sector CyberSecurity,” March 2018. [Online]. Available: https://www.energy.gov/sites/prod/files/2018/05/f51/DOE%20Multiyear%20Plan%20for%20Energy%20Sector%20Cybersecurity%20_0.pdf.

[14] Verizon Enterprise Solutions, “Verizon’s 2018 Data Breach Investigations Report,” 2018. [Online]. Available: https://www.verizonenterprise.com/resources/reports/rp_DBIR_2018_Report_execsummary_en_xg.pdf. [Accessed 16 08 2018].

[15] North American Electric Reliability Corporation (NERC), Critical Infrastructure Strategic Roadmap. Electricity Sub-Sector Coordinating Council (ESCC), 2010.

[16] Energy Sector Control Systems Working Group (ESCSWG), Roadmap to Achieve Energy Delivery Systems Cybersecurity, September 2011.

[17] L. Branscomb, P. Auerswald, T. La Porte and e. al., Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability, Cambridge, MA: Cambridge University Press, 2006.

[18] IEEE Power & Energy Society, U.S. Power and Energy Engineering Workforce Collaborative Management Steering Committee, “Preparing the U.S. Foundation for Future Electric Energy Systems: A Strong Power and Energy Engineering Workforce,” 2009. [Online]. Available: http://www.ieee-pes.org/images/pdf/US_Power_&_Energy_Collaborative_Action_Plan_April_2009_Adobe72.pdf.

5 Annex I: The CEIS-SG Group

The Critical Energy Infrastructure Security Stakeholder Group (CEIS-SG) has been established by the H2020 DEFENDER project consortium in order to guide and integrate the Energy Infrastructure sector's continuous effort, improving the security and resilience of its critical infrastructure. CEIS-SG represents a think tank and information exchange ecosystem targeting safer and more sustainable European Critical Energy Infrastructures. In particular, DEFENDER aims to initiate, via the CEIS-SG, a process to lead towards CEI security certifications, in the form of CEI Secure Tiers and DS-SLA specifications and certifications. Moreover, learning and information exchange will be promoted towards a culture of security, via wide audience communication channels, targeted industrial or scientific events, and specialized training activities. CEIS-SG is considered as a pan-European stakeholders' eco-system to define the roadmap for next generation CEI security by design and by default and to promote a Culture of CEI Security along with best practices at pan-European level.

5.1 CEIS-SG vision and goals

CEIS-SG Vision: The European Union should protect legacy CEI and design a new generation of more resilient and self-healing European Critical Energy Infrastructure able to survive large scale, combined, cyber-physical-social incidents and accidents, and guarantee the continuity of operations, while minimizing their cascading effects in the infrastructure.

The CEIS-SG will collaborate with many initiatives to address the following evolving risks & threats in CEI, also providing feedback to other critical infrastructure authorities. The main goal is to support European CEIs to:

- **Survive:** Large scale, combined, cyber-physical-social incidents and accidents;
- **Guarantee:** Continuity of operations while minimizing the cascading effects;
- **Coordinate:** Safer CEI planning/roadmap.

A side objective of the CEIS-SG is to support DEFENDER project in becoming more effective and more efficient in all activities related to CEI security. Particular emphasis will be put on communicating stakeholder requirements so that CEI security studies and the achieved results can be further developed. Indicatively: Exchange and discuss about threats, vulnerabilities and incidents, to ensure that there is a common understanding about common threats, vulnerabilities and incidents affecting Critical Infrastructures, across the EU; Give feedback on experiences with regulation and supervision to ensure effectiveness and efficiency; Point to gaps and issues that require attention from DEFENDER to ensure that important topics and issues are being addressed; Identify needs of stakeholders in the area of CEI security; Identify channels to facilitate information collection, sharing and dissemination; Identify additional elements that might be part of the CEI security.

5.2 CEIS-SG approach and working methods

CEIS-SG communication and teamwork is currently based on remote collaboration. The group is communicating offline via emails in order to fix various details, share ideas, collect and analyse requirements. In frequent time intervals (approximately every two months), a group web conference call is organized by the DEFENDER project coordinator in order to consolidated information online and conclude with decisions. In addition, periodic physical meetings are also envisaged to consider the progress at the CEIS-SG activities and the DEFENDER project.

CEIS-SG approach starts from the experience of the Smart Grid Stakeholder Group (SGSG). The SGSG was established in June 2010 to foster the information exchange between ICT and energy industry and thus to better understand each other views. The organization of the SGSG was a task in FP7 FINSENY project and the group has been open for all industrial organizations which are interested in Smart Grid/Smart Energy topics. Starting from the experience of the Smart Grid Stakeholders Group, the CEI Security stakeholder group follow a series of working methods including:

- Identify and disseminate best practices for connecting secure and resilient electricity transmission and delivery systems and business networks (e.g., deploy and properly configure firewalls, intrusion detection systems, and antivirus solutions at all appropriate locations
- Develop best practices that focus on techniques, practices, procedures, and polices for electricity sector operators, engineers, and technical staff to encourage widespread adoption
- Organize high-level meetings and workshop with relevant stakeholders (i.e. DSOs, TSOs, security agencies, EU Energy ministries secretaries executives) to gain support from the top
- Develop a roadmap to address legal aspects of collaboration, leveraging existing and forthcoming agreements and increase awareness and gain support for roadmap implementation efforts
- Develop a voluntarily populated matrix of vendors and asset owners conducting vulnerability assessments and applying best practices and measure progress of adopting certain standards and measure performance of those standards
- Establish certification procedures and methodologies towards estimation of risk and CEI Tiers classification (defined in WP1) and DS-SLAs for electricity asset owners and develop a strategic implementation plan to gain widespread adoption.

5.3 CEIS-SG Membership Benefits

The membership benefits for each category of stakeholders are summarized in Table 13.

Table 13: CEI-SG Membership Benefits per stakeholder category

Stakeholder Category	Membership benefits
CEI Owners/ Utilities	• Achieve a consensus on security issues, functionalities, operations and tools that need to be addressed to protect current and future CEI. • Share information at pan-European level on threats, incidents, countermeasures and best practices • Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe • Stay up to date on new developments, tools and commercial offerings
TSOs, DSOs, Energy companies	• Increase awareness of lurking CEI threats of assets and infrastructure • Share information at pan-European level on threats, incidents, countermeasures and best practices • Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe • Discuss emerging opportunities and shape new business models • Stay up to date on new developments, tools and commercial offerings along with funding opportunities in CEI protection
ICT & Security technology providers	• Increase awareness and feedback on opportunities regarding the joint configuration of ICT, Energy and Smart Grid for critical infrastructures. • Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe • Share information at pan-European level on CEI investment roadmap

	and stay up to date on new funding opportunities in CEI protection
Governmental, European Officials and Policy makers	• Increase awareness on CEI owners, TSOs, DSOs and Energy companies concerns, threats and standardization efforts • Contribute towards the establishment of the basis for a minimum set of auditable controls for CEI Tiers across Europe • Stay up to date on developments, research effort and commercial tools.
Law Enforcement Agencies (LEAs)	• Create awareness on potential innovative technologies able to support the territory control • Prepare the ground for shared think-tanks and/or operational units which include both CEI and LEA stakeholders • Design novel “business” or service delivery models in which LEA and CEI operators cooperate at different levels to provide CEI protection
Scientific community and industrial research in the Energy sector.	• Create awareness of the CEI current and future cyber/physical threats, research concepts and the vision for the future secure by design CEI. • Stay up to date on new research and developments along with funding opportunities in CEI protection