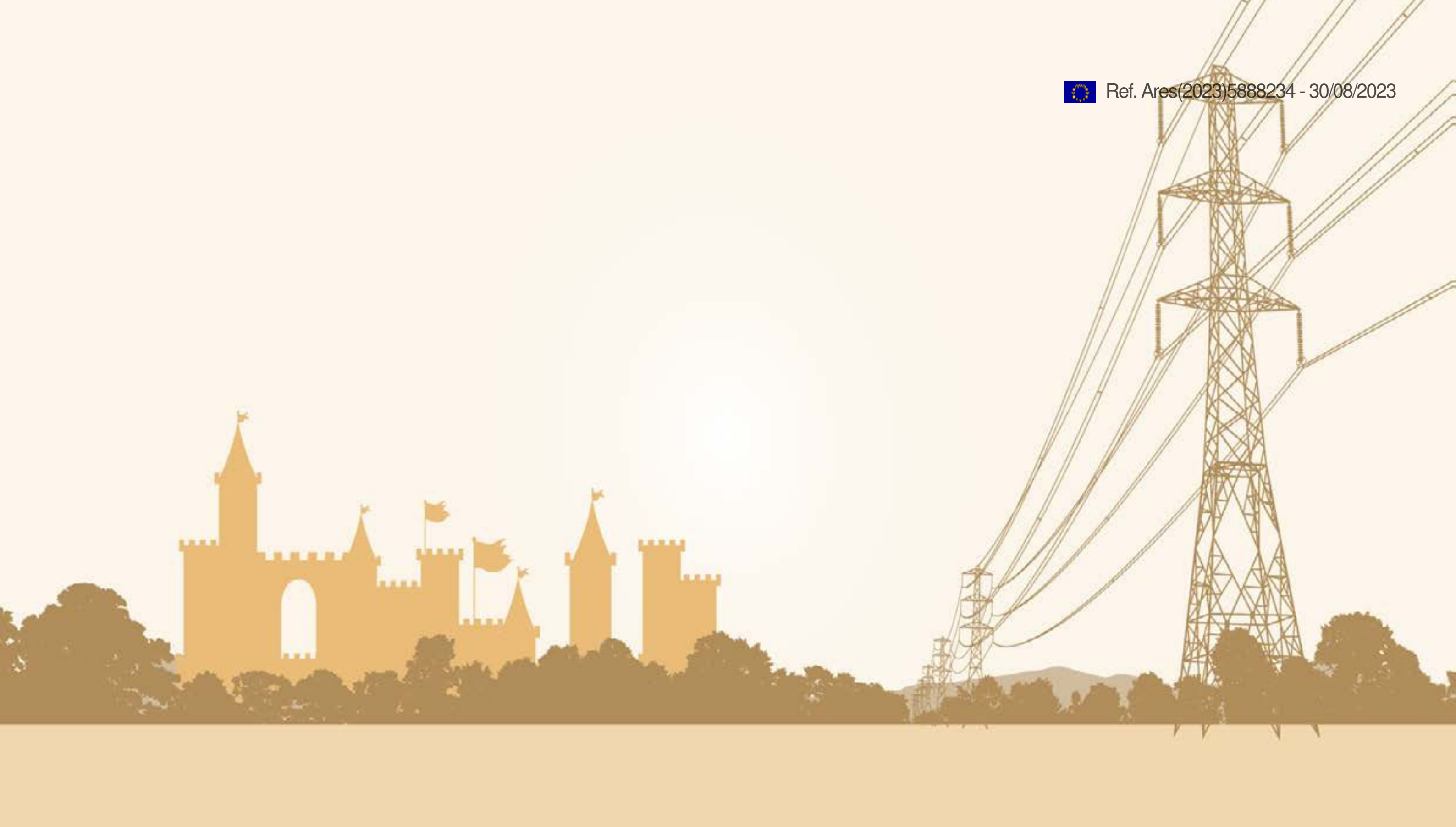


Establishment of a FramewORk for Transforming current EPES into a more resilient, reliable and secure system all over its value chain

Cascading Effects Analysis and Related Actions to Increase Resilience

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Document details

Deliverable no	D2.2
Deliverable name	Cascading effects analysis and related actions to increase resilience
Version	1.0
Release date	29/8/2023
Type	R
Dissemination level	PUB
Status	Final version
Authors	TUD – Ali Mollaiee, Mehran Hashemian, Alexandru Stefanov RINA-C – Saimir Osmani, Fabio Bolletta TNO – Luca Morgese, Frank Fransen FRAUNHOFER – Sebastian Ganter, Jörg Finger COMILLAS – Néstor Rodríguez, Gregorio López, Javier Matanza, Lukas Sigrist, Miguel Ángel Sánchez Fornié ENCS – Elvira Sánchez Ortiz HYPERTECH – Christopher Ververidis, Despina Brasinik, Maria Toupadaki SCHN – David Pampliega CIRCE – Marta Bernal Sancho CERTH – Pashalis Gkaintatzis

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

DISCLAIMER OF WARRANTIES

This document has been prepared by eFORT project partners as an account of work carried out within the framework of the EC-GA contract no. 101075665.

Neither Project Coordinator, nor any signatory party of eFORT Project Consortium Agreement, nor any person acting on behalf of any of them:

a) makes any warranty or representation whatsoever, expressed or implied,

   I. with respect to the use of any information, apparatus, method, process, or similar item disclosed in this document, including merchantability and fitness for a particular purpose, or

   II. that such use does not infringe on or interfere with privately owned rights, including any party's intellectual property, or

   III. that this document is suitable to any particular user's circumstance; or

b) assumes responsibility for any damages or other liability whatsoever (including any consequential damages, even if the Project Coordinator or any representative of a signatory party of the eFORT Project Consortium Agreement has been informed of the possibility of such damages) resulting from your selection or use of this document or any information, apparatus, method, process, or similar item disclosed in this document.

This work has been Funded by the European Union. Views and opinions expressed are however those of the author(s) only and do not necessarily reflect those of the European Union or the European Climate, Infrastructure and Environment Executive Agency (CINEA). Neither the European Union nor the granting authority can be held responsible for them.

Document history

Version	Date of issue	Content and changes	Edited by
0.1	19/04/2023	Table of contents	TUD
0.2	25/07/2023	First draft	TUD
0.3	10/08/2023	Second draft	TUD
0.4	17/08/2023	Peer revision	CIRCE, CERTH, ENCS, TENNET
0.5	23/08/2023	Final version	TUD
0.9	29/08/2023	Final quality check	CIRCE
1.0	31/08/2023	Final version	TUD

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Table of content

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

List of figures

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

List of tables

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Abbreviations and Acronyms

Acronym	Description
AC	Alternating current
ARP	Address Resolution Protocol
BB	Building Block
BoM	Bills of Materials
CoA	Courses of Actions
COSMIC	Cascading Outage Simulator with Multiprocess Integration Capabilities
CPS	Cyber-Physical Systems
CSIRT	Computer Security Incident Response Team
DC	Direct Current
DFIG	Doubly-Fed Induction Generator
DNS	Domain Name System
DoS	Denial-of-Service
DPC	Delta Power Control
DR	Demand Response
ENTSOE	European Network of Transmission System Operators for Electricity
EPES	Electrical Power and Energy System
ERCOT	Electric Reliability Council of Texas
EV	Electric Vehicle
EVCS	Electric Vehicle Charging Stations
FACTS	Flexible AC Transmission System
FCR	Frequency Containment Reserve
FDIA	False Data Injection Attack
FFT	Fast Fourier Transform
GSA	GPS Spoofing Attack
HV	High Voltage
HVDC	High-Voltage DC
IACS	Industrial Automation and Control System
IoT	Internet of Things

Acronym	Description
ISMS	Information Security Management System
IT	Information Technology
LAA	Load Altering Attack
LV	Low Voltage
Medio	Manipulation of Demand through IoT
MISO	Midwest Independent System Operator
MITM	Man-in-the-Middle
MPM	Matrix Pencil Method
MV	Medium Voltage
NERC	North American Electric Reliability Corporation
NIAC	National Advisory Council
OT	Operational Technology
PMU	Phasor Measurement Unit
PoC	Points of Contact
PSI	Power System Stabilizer
PV	Photovoltaics
QSS	Quasi-Steady-State
RA	Risk Assessment
RES	Renewable Energy Sources
ROCOF	Rate of Change of Frequency
SCADA	Supervisory Control and Data Acquisition
SDN	Software Defined Networking
SGAM	Smart Grid Architecture Model
SI	Synthetic Inertia
SOAR	Security Orchestration, Automation, and Response
SOC	Security Operations Centre
SSR	Sub-Synchronous Resonance
TRELSS	Transmission Reliability Evaluation of Large Scale Systems
TSO	Transmission System Operator
UFLS	Under Frequency Load Shedding scheme

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Acronym	Description
WPP	Wind Power Plant
WSCC	Western System Coordinated Council

Definition of important terms

Term	Definition
Risk	Risk is the possibility of an undesired event and its sequenced loss.
Hazard	A hazard is an event or set of events that is the source of potential damage. Hazards cause concerns for system owners and operators.
Vulnerability	Vulnerability is a condition or a process resulting from a given (natural or man-made) hazard and is defined as the joint conditional probability distribution of hazard likelihood, hazard potential impact and system capacity.
Resilience	The resilience of a system presented with an unexpected set of disturbances is the system's ability to reduce the magnitude and duration of the disruption. A resilient system downgrades its functionality and alters its structure in an agile way.
Reliability	Reliability is the ability of the power system to deliver electricity to customers with acceptable quality and in the amount desired while maintaining grid functionality even when failures occur.
Stability	Stability is the ability of a system to remain intact after being subjected to small perturbations.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Executive summary

Modern power systems, characterized by high renewable energy penetration and advanced digital technologies, face various risks of failures caused by disturbances and disruptions. The uninterrupted supply of electricity is vital for essential aspects of the modern society, including healthcare, communication, transportation, and more. Hence, ensuring Electrical Power and Energy System (EPES) resiliency and reliability are paramount to uninterrupted electricity supply. This report aims to assist system operators in achieving this goal by providing a thorough analysis of cascading failures and proposing effective actions to improve system resilience. The content of this report is based on the research and studies conducted in tasks T2.3, T2.4, and T2.2, and its findings can be applied in task T4.3 to defend against cascading failures and develop self-healing capabilities.

The report delves into understanding the critical problem of cascading failures within modern power systems. It examines pre-conditions and initiating events, investigating the main stages and underlying mechanisms of cascading failures. Identifying critical factors contributing to cascading failures, which can be exploited by cyber-attacks, forms an important part of this study. Subsequently, the report investigates how cyber-attacks can initiate or accelerate cascading failures, considering the critical factors. To demonstrate the impact of cyber-attacks on power system operation, which may cause cascading failures, the report employs simulation scenarios, including load-altering attacks on Electric Vehicle (EV) charging stations and Manipulation of Demand through IoT (MadIOT) attacks.

The latter part of the report introduces two main groups of actions to enhance resilience and minimize economic losses in modern power systems. These strategies are categorized into the physical and cyber layers. By implementing these measures, power systems can better be safeguarded against potential disruptions, reinforcing their stability and reliability.

In conclusion, this report provides a comprehensive analysis of cascading failures in modern power systems and potential risks posed by cyber-attacks. The proposed resilience strategies offer practical measures to improve system resiliency, considering both cyber and physical layers. By adopting these strategies, power systems can better cope with challenges, ensuring the continuous electricity supply to support the modern society. This report serves as a resource for system operators, policymakers, and researchers working towards a more robust and secure power grid.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

1 Introduction

The uninterrupted electrical energy supply is crucial to various critical infrastructures, such as transportation, telecommunication, water management systems, healthcare services, and information technology. Consequently, disruptions in electricity supply can significantly affect the quality of people's lives (H. Guo et al., 2017). As complex systems, power grids are essential in generating, transmitting, and distributing electricity. Therefore, ensuring the power system's reliability and security is pivotal for the secure grid operation and uninterrupted energy supply (Sharma et al., 2021). However, power systems can encounter numerous faults and failures due to their vast geographical coverage. Furthermore, with the growing demand for energy and the integration of renewable energy resources, modern power systems operate close to their stability margin, making them vulnerable to critical disturbances (Haes Alhelou et al., 2019).

These disturbances can threaten the balance between electricity supply and demand and affect power system stability. They can lead to power outages that can disrupt the modern society. Widespread outages, commonly known as blackouts, have profound economic and social consequences, affecting various aspects of our lives. While natural disasters like earthquakes or floods can cause widespread blackouts, cascading failures have played a pivotal role in creating a large-scale blackout, as was observed in many historical cases. Due to the deep interdependency among power grid components, the outage of a single component, such as a transmission line, can trigger subsequent failures propagating throughout the system. Consequently, these failures push the power system to a critical condition where it cannot maintain stability, resulting in an uncontrollable disconnection of power elements and a blackout (Pourbeik et al., 2006).

The increasing penetration of renewable energy sources introduces higher interdependencies among regions, elevating the risk of cascading failures. Moreover, power electronic converters increase the system complexity by adding more dynamics to the power system, raising the probability of component failures. Hence, it is imperative to thoroughly examine cascading failures within modern power systems with a high degree of renewable energy integration. On the other hand, the emergence of digital technologies such as digital substations, Phasor Measurement Units (PMUs), artificial intelligence, and advanced energy management systems has amplified the significance of the cyber layer in power system stability and control. Accordingly, failures within the cyber system may also result in power outages. Of more significant concern, cyber-attacks have the potential to profoundly impact power system operation by instigating or accelerating cascading failures. Therefore, conducting an in-depth investigation of cascading failures is essential for discovering the underlying mechanisms behind these critical disturbances.

Furthermore, identifying solutions to improve system resilience and minimize economic losses resulting from both physical and cyber disruptions is paramount in ensuring the secure electricity supply. The mitigation solutions are categorized into resilience actions at the physical and cyber layers. By implementing the resilience measures, the power grid can be better safeguarded against cascading failures and power outages, reinforcing power system stability and reliability. Ultimately, these efforts ensure that electricity continues to serve as a dependable cornerstone of the modern society.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

In summary, this report presents a comprehensive analysis of cascading effects along with effective actions to increase power system resilience and mitigate the detrimental effects of disruptions in electricity supply. In order to achieve this objective, this report starts by investigating major blackouts over the past two decades worldwide. It analyses the cascading failure mechanisms and identifies the critical factors associated with each incident. The output of this analysis is subsequently utilized to outline a general overview of cascading failures in power systems. This overview covers the key stages of cascading effects, i.e., pre-condition, initiating events, slow cascade, point of no return, fast cascade, blackout, and system restoration. Furthermore, this report investigates the underlying mechanisms and identifies critical factors contributing to the propagation of failures. The link between the critical factors and cyber-attacks is investigated. Simulation scenarios are conducted to analyse the impact of cyber-attacks on power system operation. Resilience actions are proposed at both cyber and physical system layers to increase power system resilience and minimize economic losses.

2 Analysis of cascading effects

2.1 Anatomy of a power grid blackout: root causes and mechanisms

Power grid operators face numerous complex challenges in ensuring the reliability and resilience of power systems. Among these challenges, cascading failures represent an unsolved problem that poses a significant risk to the reliability and resiliency of power systems, potentially leading to a blackout. Modern power systems are intricate and interconnected, containing multiple subsystems. In such a highly integrated and interdependent system, ensuring the reliability and resilience of the energy supply under all operating conditions becomes unfeasible. Various unseen interdependencies and hidden interactions between power grid components make anticipating the system's response difficult.

Furthermore, integrating renewable energies, demand response programs and power electronic converters in power systems introduces additional complexity and interdependency, making power systems more vulnerable to cascading failures. Therefore, revealing the underlying cascading failure mechanisms is paramount for power grid operators. Accordingly, a coherent vision of cascading failure phenomena with in-depth details of the underlying mechanism is essential for proactively identifying and effectively mitigating their consequential impacts.

Moreover, power systems' extensive geographical area makes them susceptible to various failures and disturbances, which can trigger a chain of cascading effects. Given the high occurrence rate of these events and the complexity of modern power systems, understanding cascading failures becomes even more critical. Consequently, it is vital to identify the root causes of cascading events and uncover the general patterns and key stages of blackouts.

2.1.1 Root causes of cascading failures

Power systems are subject to diverse threats and disturbances. Understanding the origins of these disturbances is the first step in revealing the underlying mechanisms behind the cascading failures and blackouts. These disturbances can push the power system into an emergency state or even initiate a series of failures that potentially result in a blackout. Various factors, often called root causes, contribute to these disturbances within the power system. External root causes predominantly originate from outside the power grid, encompassing weather conditions or physical damage caused by animals or external forces. Conversely, internal root causes primarily stem from factors within the power system, such as equipment malfunctions or control system issues.

2.1.1.1 External root causes of disturbances

External factors refer to events or conditions outside the power system and can contribute to cascading failures by causing disturbances. Some examples of external factors that can contribute to cascading failures include:

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

1. Natural disasters

Natural events have been one of the key disturbance sources in power systems. Due to their vast geographical range, power grids are always susceptible to extreme weather conditions (Wang et al., 2016). Natural disasters such as storms, floods, earthquakes, and wildfires can damage power system infrastructure, causing equipment failures and initiating cascading failures.

2. Cyber-attacks

In recent years, with the growing trend of digitalization in power systems, operational technologies have been exposed to numerous threats, increasing the risk of cyber-attacks. Accordingly, malicious attacks can target various applications in the power system, including substation control, wide-area monitoring, Supervisory Control and Data Acquisition (SCADA), and energy management systems. In this case, if an intruder exploits the system's vulnerabilities, it can cause an outage or even instigate a cascading chain of outages (Sun et al., 2018).

3. External interdependencies

Power systems are interconnected with other major infrastructures and systems, such as communication, transportation, and gas supply systems. Failures in these external systems can lead to cascading failures due to system interdependencies. Moreover, factors such as the energy market can also affect the power grid and accelerate cascading failures in different ways, e.g., changes in demand and supply (B. Li & Sansavini, 2017).

4. Other disturbances

Root causes of cascading failures are not limited to these factors. Many unknown disturbances, such as unintended physical damage by animals or deliberate damage, can cause outages and facilitate the conditions for cascading failures (Sharma et al., 2021).

2.1.1.2 Internal root causes of disturbances

Internal factors refer to events or conditions within the power system that can disrupt its functioning and result in cascading failures. Examples of internal issues that have the potential to trigger cascading failures include the following:

1. Equipment failures

Power grids are large complex systems with various components and subsystems such as generators, transmission lines, and transformers. In such a large system, component failure is inevitable, weakening the system's reliability. As a result, critical equipment failure can trigger a chain reaction of failures in other parts of the power system.

2. Human error

Since humans have the main responsibility in power system operation and control, human error can significantly jeopardize the power system operation. For example, if the operator fails to respond to a failure properly, it may cause a chain of failures and lead to a blackout.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

3. Malfunctions in control and protection systems

Control and protection systems are pivotal in maintaining power system stability. As a result, failure in these systems, e.g., relay malfunction, can threaten power system stability and push the power grid to emergency conditions, where the system is vulnerable to other component failures. Consequently, if the equipment fails in such circumstances, the system cannot respond adequately, and the power system will be exposed to cascading failures.

4. Inadequate monitoring and control systems

Detecting and responding to disturbances can be challenging without adequate monitoring and control systems. Hence, real-time monitoring and control are crucial for grid operators to absorb the shock and prevent cascading failures. Moreover, in case of cascading failures, advanced monitoring and control systems can aid operators in mitigating cascading effects and restoring the system to normal operating conditions (Chadwick, 2013).

2.1.2 Overview of cascading failures

A comprehensive understanding of cascading failures requires a general overview capturing key stages which are crucial for uncovering the underlying mechanisms. In most historical incidents, cascading failures originate from a single system failure. Subsequently, this failure triggers a domino effect, pushing the system toward its stability margin. Eventually, the system enters extreme conditions, where protective relays trip critical equipment. A large mismatch between the load and generation will happen in such circumstances, causing uncontrolled islanding. Ultimately, the system cannot supply loads and faces a widespread blackout. Figure 1 provides a clear and abstract representation of cascading failures and their progression toward a blackout based on historical incidents. However, this depiction lacks specific details regarding the system status and mechanisms underlying the propagation of failures.

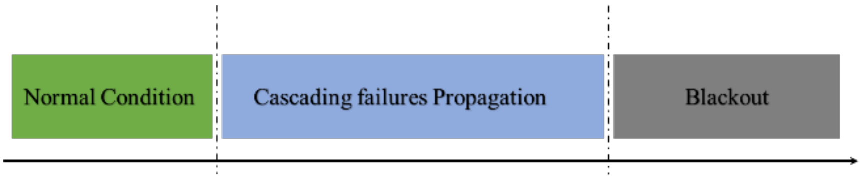


Figure 1. Simple blackout timeline

To thoroughly understand cascading failures, it is essential to consider the power system's operating conditions at each stage before and after the blackout. Additionally, investigating the roles of stability and protection in the propagation of failures is crucial for comprehending the system's response during each event. Figure 2 presents a generalized timeline that outlines the key stages of cascading failures, serving as a foundational framework for this report's subsequent discussion on cascading failures.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

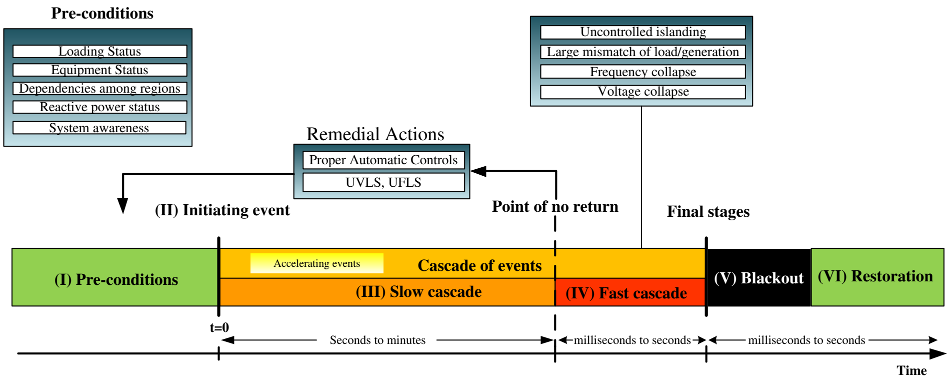


Figure 2. Key stages of cascading failures

The figure shows that the timeline includes six main stages: pre-condition, initiating event, slow cascading failures, point of no return, fast cascading failures, and blackout. A brief description of each stage is provided as follows.

1. Pre-condition

This stage refers to the operating conditions and the status of the power system before the domino effect of failures starts. In this stage, the power system is operated normally, and all loads are fully supplied. However, systems may be subject to cascading failures due to the stability status, overload situation, or maintenance of some critical components. A thorough analysis of pre-conditions will allow the operator to anticipate the cascading failures' occurrence in advance.

2. Initiating event(s)

Typically, a failure or disturbance, like a short circuit, triggers the chain of events in the system. The power system is exposed to abnormal conditions.

3. Slow cascade

The domino effect of cascading failures starts at this stage. It is worth noting that the propagation of cascading failures is a complicated process influenced by many factors. In the first phase of cascading failures, the rate of outages is relatively slow, called "slow cascade." In this stage, a failure of one component exacerbates the situation and pushes the power system closer to its stability margin. Throughout this process, protective relays operate to maintain the system's stability. Nevertheless, as more components are tripped, the security margin of the system will be decreased, ultimately leading the system into an emergency state. Understanding this stage will help the operator to take appropriate preventive and corrective action to stop the progression of failures.

4. Point of no return

This point divides cascading failure propagation into two phases: slow and fast. After this point, preventive and corrective actions cannot mitigate cascading effects effectively, and the power system is exposed to extreme conditions with a high risk of collapse and a blackout.

5. Fast cascade

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

The fast cascade stage represents a critical stage within the cascading failure process, characterized by severe disruptions in voltage and frequency within the power system. During this stage, the stability margin of the system becomes significantly diminished, making it challenging to maintain stability. Consequently, the protective relays trip various components in the system and try to ensure the balance between demand and generation by load shedding. However, if the protection schemes and islanding procedures are inadequately designed to address cascading failures, uncontrolled islanding can occur, causing voltage and frequency collapse.

6. Blackout

After voltage and frequency collapse, the system enters a blackout stage where most of the generation is lost. In this case, a detailed power system restoration strategy should be implemented to recover the power system.

2.2 Historical blackouts around the world

In this section, the study delves into the analysis of significant historical blackouts, aiming to reveal the mechanism behind the propagation of cascading failures and the severity of blackouts. Table 1 shows some substantial power outages in the last two decades including affected number of people for each event. By examining these specific instances, a clearer understanding of the cascading failures mechanism can be gained and derive lessons for mitigating their impact in the future. A detailed description the major blackouts can be found in Annex II: Analysis of cascading failures.

Table 1. People affected by blackouts

Date	Country	People affected	Origin
March 2015	Turkey	70.000.000	Technical problem at TSO
January 2015	Pakistan	140.000.000	Militant attack
July 2012	India	620.000.000	Overload
February 2008	USA (Florida)	6.000.000	Transformer station
July 2007	Spain (Barcelona)	350.000	Defective switchgear
July 2007	Georgia	1.100.000	
November 2006	Germany / NW Europe	10.000.000	
November 2005	Germany	250.000	Buckling pylons
May 2005	Russia (Moscow)	2.000.000	
November 2004	Spain	2.000.000	Fire in transformer
September 2004	Germany (Rheinland-Pfalz)	1.000.000	Short – circuit
December 2003	Germany (Gutersloh)	300.000	Sabotage

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

September 2003	Sweden /Denmark	4.000.000	Switching error
September 2003	Italy	56.000.000	Breakdown of high-voltage line
August 2023	USA / Canada	50.000.000	Computer error
June 2003	Italy	6.000.000	Insufficient capacity
January 2001	India	200.000.000	

Table 2 is focused mainly on social impacts such as the number of end-users, blackout duration, energy not supplied, and disruption estimated cost (Bompard, E. et al., 2011).

Table 2. Blackout social impacts

Country	**Social impacts**		
	N° of end-users interrupted	**Duration, energy not supplied**	**Estimated costs to the whole society**
Sweden/Denmark, 2003	0.86 million (Sweden) and 2.4 million (Denmark)	2.1 hours, 18 GWh	145 – 180 M€
France, 1999	1.4 – 3.5 million, 193 million m^3 wood damaged	2 days – 2 weeks; 400GWh	11.5 bn€
Italy / Switzerland, 2003	55 million	18 hours	
Sweden, 2005	0.7 million, 70 million m^3 wood damaged	1 day – 5 weeks; 111GWh	400 M€
Central Europe 2006	15 million	< 2 hours	

2.3 Assessment of pre-conditions and initiating events

As discussed in section 2.1, the general mechanism behind the cascading failures and blackout entails a complicated phenomenon. Figure 2 shows the general sequence of stages leading to a blackout. Analyzing previous historical cascading failures around the world reveals that different pre-conditions and initiating events affect the cascading failure mechanism, which is not well-addressed so far. Therefore, this section aims to identify these pre-conditions and initiating events and investigate their effect on the cascading failure sequence. According to Figure 2, before initiating a succession of failures in the power system, the pre-condition and initiating event should be regarded as influential stages in the chain of cascading failures. This report analyzes 13 major historical cascading failures and blackouts to identify the main pre-conditions and initiating events.

2.3.1 Pre-conditions

Among all pre-conditions analyzed through historical blackouts, loading status, equipment status, dependencies between regions, reactive power status, and system awareness are selected as influential pre-conditions. Table 5, in Annex II: Analysis of cascading failures, shows the pre-conditions for major historical blackouts around the world. In the subsequent sections, each identified pre-condition will be discussed in detail, providing insights into their impacts on cascading failures in power systems. By analyzing major historical blackouts, how these pre-conditions manifested in real-world scenarios and contributed to the severity of cascading failures is examined. The objective is to gain a comprehensive understanding of the role played by each pre-condition in the occurrence and propagation of blackouts, thereby enhancing the knowledge of the underlying mechanisms and improving the resilience of power systems. Additionally, analyzing specific historical blackouts will help illustrate the practical implications of these pre-conditions and provide valuable lessons for future power system planning and operation.

2.3.1.1 Loading status

Generally, a power system's loading status refers to the electrical demand level and corresponding supply capacity available within the system. It plays a crucial role as a pre-condition in cascading failures and blackouts. High-loading conditions significantly stress the power grid infrastructure and reduce the system's flexibility, increasing the likelihood of voltage fluctuations, system instability, and vulnerability to disturbances (Kundur & Balu, 1994). During periods of peak demand or when the system is operating close to its maximum capacity, even minor disruptions or unexpected events can propagate rapidly, triggering a cascade of failures throughout the network (Rzysztof & Roka, 2019). On the other hand, with the increased penetration of renewable energy resources, power systems face significant issues from excess energy derived from these sources during normal and off-peak periods. In this case, the system may face low inertia issues, reactive power imbalance, and inadequate reserve capacity that may lead to cascading failures. Such failures can disrupt the balance between generation and demand, leading to voltage collapse, frequency deviations, and eventual blackouts (Sanjeev et al., 2018). Figure 3 provides a visual summary of the findings presented in Table 5 regarding the loading status. According to this figure, most recent blackouts occur in normal and off-peak loading conditions. Therefore, it is essential for power system operators to investigate the possibility of cascading failures not only during high-loading conditions but also in normal and off-peak situations.

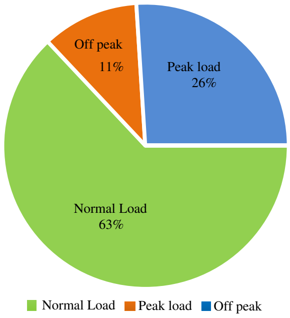


Figure 3. Distribution of blackouts occurrence in different loading statuses

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

2.3.1.2 Equipment status

The equipment status within a power system is another crucial pre-condition that can significantly impact the occurrence and severity of cascading failures and blackouts. Planned outages and unplanned events, such as short circuits or equipment failures, exert substantial stress on the power infrastructure and reduce the system's overall flexibility. Planned outages involve intentional equipment outages for maintenance, repairs, or upgrades. While necessary for ensuring the system's long-term reliability, these outages can create vulnerabilities by reducing the available capacity and alternate paths for power flows. Similarly, unplanned events like short circuits or equipment failures can trigger sudden disruptions, leading to imbalances in the power flow and potentially propagating failures throughout the network. These events increase the likelihood of system instability and reactive power demand, causing excitation problems and decreasing the power system's ability to absorb and recover from disturbances. Therefore, when analyzing historical cascading failures and blackouts, it is essential to consider the effect of equipment status on the propagation of cascading failures and the severity of blackouts. Understanding the vulnerabilities associated with planned and unplanned equipment outages is crucial for enhancing the resilience and reliability of the power system. Figure 4 illustrates the occurrence of blackouts categorized by different equipment statuses, emphasizing the significance of generators and transmission line outages on the occurrence of cascading failures and blackouts. According to this figure, most historical blackouts experienced planned or unplanned outages before initiating a sequence of failures.

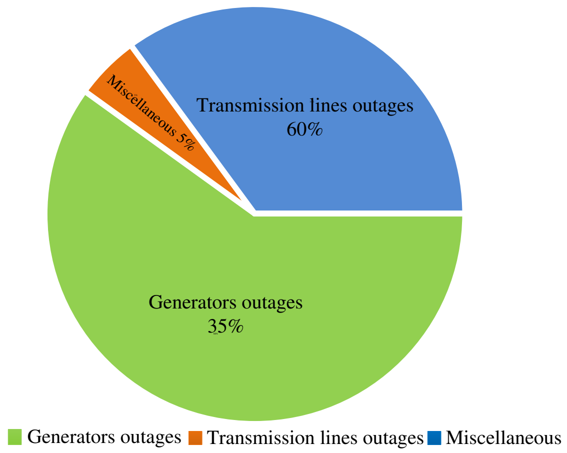


Figure 4. Distribution of blackouts occurrence in different equipment status

2.3.1.3 Dependencies between regions

The dependency between regions within a power system is a critical pre-condition that can significantly influence the occurrence and propagation of cascading failures and blackouts.

When regions have a high level of interdependency, disruptions or failures in one region can be quickly propagated through interconnected transmission lines and affect neighboring regions. This interdependency can create a domino effect, where a failure in one region burdens the neighboring regions, potentially leading to a widespread cascade of failures. Historical blackouts provide evidence of the detrimental impact of high regional dependency on the power system's stability and resilience. During such

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

events, failures originating in one region triggered failures in interconnected regions, exacerbating the severity and extent of the blackout. Analyzing these historical blackouts highlights the importance of understanding and managing the dependencies between regions to mitigate the risk of cascading failures. Implementing measures such as enhanced coordination, robust contingency plans, and improved interregional communication can help reduce the vulnerability of the power system to interdependent failures and strengthen its overall resilience. Figure 5 depicts the status of the dependency among the regions in historical blackouts. According to this figure, most historical blackouts experienced high dependency among their regions.

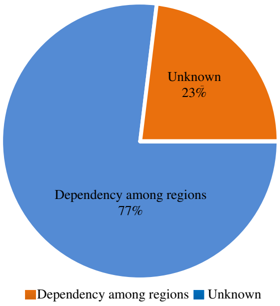


Figure 5. Distribution of blackouts occurrence based on dependencies between regions

2.3.1.4 Reactive power status and system awareness

The availability of reactive power reserves and management of power flows, coupled with an awareness of these factors, are crucial pre-conditions in preventing cascading failures and blackouts within power systems. Reactive power reserves, which are the reserves of reactive power that can be quickly supplied or absorbed by power system components, play a vital role in maintaining voltage stability and ensuring the reliable operation of the system. Insufficient reactive power reserves can lead to voltage collapse and impair the ability of the system to respond to sudden changes in load or disturbances. This can set off a chain of events, causing cascading failures that propagate through the network and result in a blackout. For instance, the Pacific Southwest blackout on 8th September 2011 is an example of inadequate reactive power reserves contributing to cascading failures and subsequent blackouts in the region. Similarly, power flow mismatches and a lack of awareness of system conditions can exacerbate the risk of cascading failures. Power flow mismatch refers to the imbalance between power generation and demand, often caused by unplanned outages, equipment failures, or inadequate transmission capacity. Insufficient awareness of these mismatches and resultant stress on the system can impede timely intervention and necessary corrective actions. The U.S.-Canadian blackout on 14th August 2003 and the India blackout on 30th July 2012 highlights the consequences of power flow mismatch and lack of awareness, where the cascading failures originated from a local disturbance but quickly spread out due to a lack of awareness and coordination, resulting in a large blackout affecting multiple regions. Understanding the theoretical aspects of reactive power reserves, power flow mismatches, and the importance of awareness is essential for preventing cascading failures and blackouts.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

2.3.2 Initiating events

Initiating events are disturbances that trigger the cascade of events on the power systems. These events serve as triggers that initiate a chain of failures, leading to the propagation of disruptions across the network. Understanding and analyzing these initiating events is crucial for comprehending the dynamics of cascading failures and devising effective mitigation strategies. Initiating events can encompass a range of factors, including short-circuit faults, overloads, hidden protection failures, and other critical incidents. Each event plays a distinct role in cascading failure propagation. Therefore, this section will delve into the importance of these initiating events and their impact on cascading failures.

Table 6 in Annex II: Analysis of cascading failures presents the identified initiating events responsible for significant historical blackouts worldwide. In the following sections, these identified initiating events are discussed, providing detailed discussions that shed light on their influence on cascading failures within power systems.

2.3.2.1 Short-circuits

The occurrence of cascading failures caused by short circuits, even in the presence of N-1 and N-2 contingencies, highlights the complexity and vulnerability of power systems. Despite robust contingency plans aimed at maintaining system reliability, short circuits possess the potential to disrupt the balance of electrical currents and overwhelm protective measures. A short circuit resulting from a fault or abnormal current path with reduced resistance can induce excessive current flow and impose immense stress on nearby components. In some cases, this stress exceeds the capacity of protective devices and contingency measures, leading to the failure of multiple interconnected components. Consequently, the failure cascade initiated by a short circuit can propagate through the network, bypassing the safeguards provided by N-1 and N-2 contingencies. Understanding the underlying mechanisms and exploring strategies to enhance the resilience of power systems against such cascading failures caused by short circuits is crucial for maintaining a reliable and secure electricity supply.

2.3.2.2 Overload

Overloads pose a significant risk to power grids and can act as initiating events for cascading failures with severe consequences. Various factors contribute to the occurrence of overloads, including increased power demand, transmission line congestion, generation capacity limitations, and unforeseen disruptions in the network. When the power demand surpasses the capacity of the electrical infrastructure, components such as transmission lines, transformers, and other equipment experience excessive heat buildup and stress, these events can disrupt the balance between power generation and consumption, pushing the system toward an overloaded state. Once an overload occurs, the consequences can be severe. The excessive thermal stress on components can lead to their degradation or failure, triggering protective mechanisms such as relays and circuit breakers to operate. However, in cases where protective devices are overwhelmed, or their coordination is compromised, the overload can propagate to neighboring components, triggering a chain reaction of failures and potentially escalating into a cascading failure scenario.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

2.3.2.3 Hidden protection failures

Protection systems play a critical role in power grids by detecting and isolating faults to prevent their propagation and minimize disruptions. However, protection systems themselves can sometimes experience hidden failures, which can have significant implications for the stability and reliability of the grid. Hidden protection failures occur when protective devices, such as relays or circuit breakers, fail to operate as intended during fault conditions. These failures can be attributed to various reasons, including improper calibration, inadequate maintenance, misconfiguration, software bugs, communication failures, or even human errors. Hidden protection failures increase the likelihood of faults not being promptly detected, leading to their propagation and the escalation of cascading failures. The impact of protection hidden failures on cascading failures and the severity of blackouts is substantial. When protective devices fail to operate correctly, faults can go undetected or isolated, allowing them to spread through the network. This can lead to an uncontrolled propagation of failures, affecting a larger portion of the grid and increasing the severity of blackouts. Additionally, compromised protection systems can result in incorrect or delayed responses to faults, further exacerbating the cascading effects and impeding the restoration process.

2.3.2.4 Other initiating events

In addition to short circuits, overloads, and hidden protection failures can contribute to cascading failures. These include equipment failures, human errors, and cyber-attacks. Each event possesses its unique characteristics and potential implications for the cascading failure mechanisms.

2.4 Cascading failures mechanisms

In interconnected and modern power systems, cascading failures pose a real and alarming threat, capable of triggering blackouts and significantly impacting the modern society. Consequently, it becomes crucial to fully comprehend the underlying mechanisms behind these cascading failures to effectively mitigate their potential consequences, particularly in the event of cyber-attacks. This section first serves to investigate the significance of power system stability in the system response. The power system contains diverse components and sub-systems characterized by specific time scales and attributes. Consequently, it becomes essential to thoroughly examine stability phenomena and their potential contribution to the propagation of cascading failures. Subsequently, with a solid understanding of stability, the general mechanism driving the propagation of cascading failures is analyzed. To this end, the role of the protection system is initially discussed. Following that, the investigation delves into the identification and analysis of general critical scenarios that prominently contribute to cascading failures.

2.4.1 The role of power system stability

Power systems are susceptible to a wide range of disturbances, both small and large. Small disturbances, such as load fluctuations and changes in renewable energy resources, occur frequently and can affect operating conditions. On the other hand, large

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

disturbances, including short circuits or loss of generators, significantly impact the whole power system. Maintaining power system stability is crucial in such situations to adapt to changing conditions and ensure a secure and reliable grid operation. Basically, power system stability refers to the ability of a power system to reposition from a pre-disturbance operating equilibrium point to a post-disturbance operating equilibrium point where most system variables are within their allowable ranges (Kundur et al., 2004).

Since power system failures directly impact stability, maintaining an adequate stability margin is essential to withstand cascading failures and mitigate their effects. The response of the system and the new equilibrium point depend on various factors, such as the duration and location of the failure, the nature of the failure, and the system's pre-condition. In this regard, it is necessary to obtain a clear vision of power system dynamic behavior to understand the mechanism behind cascading failures and identify general phenomena.

A typical power system is a high-order multivariable process whose dynamic response is influenced by various components, including generators, loads, and transmission lines. As a result, the anticipation of system response and stability evaluation is challenging for grid operators due to the high nonlinearity and uncertainty of power grids. Moreover, modern power systems have evolved thoroughly due to new emerging technologies for integrating renewable energies, such as voltage source converters (L. Xiong et al., 2022). These new components with different characteristics and response rates affected the dynamic behaviors of the system, making it more complex and intricate. The aforementioned stability definition considers the interconnected power system as an integrated whole. Often, however, the main interest in the research is the stability of generators as critical components in power systems, including high-order dynamic models. Similarly, the stability of other particular components in a system, like motors or groups of power electronic converters, is also a focus area for researchers. Nevertheless, both views can be applied to this study; the high-level system stability is analyzed to provide useful information about the system's current state and stability margin. Conversely, component-oriented stability is also essential in cascading failure analysis because it can help to comprehend the equipment’s dynamic response in case of disturbances.

Table 3. Impact of instability phenomena on each stage

Stage	Short-term voltage instability	Long-term voltage instability	Short-term frequency instability	Long-term frequency instability	Rotor angle transient stability	Rotor angle small signal stability	Torsional resonance	Electrical resonance	Slow converter-driven stability	Fast converter-driven stability
Initiating events	High	High	Low	High	High	Medium	Low	Low	Low	Low
Slow cascade	Medium	High	Medium	High	Low	High	Medium	Medium	Medium	Low

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Stage	**Short-term voltage instability**	**Long-term voltage instability**	**Short-term frequency instability**	**Long-term frequency instability**	**Rotor angle transient stability**	**Rotor angle small signal stability**	**Torsional resonance**	**Electrical resonance**	**Slow converter-driven stability**	**Fast converter-driven stability**
Fast Cascade	High	Low	High	Low	Medium	Medium	Medium	Medium	Medium	High

Table 3 summarizes the impact of each instability occurrence in three critical stages of cascading failures. Based on this table, voltage and frequency stability play the most influential role in propagating cascading events. Furthermore, the new stability phenomena driven by power electronics can contribute to the system's response in fast cascading failures. It is worth mentioning that although the rotor angle stability is essential in power system dynamics, it may not harshly affect the power system due to the high stability margin.

A detailed discussion about the power system stability can be found in Annex II: Analysis of cascading failures.

2.4.2 The role of protection schemes

The main objectives of protection schemes in power systems are to detect and isolate faults promptly and keep the power system stable. In this regard, if part of the power system deviates from the normal operating condition, then protection schemes should bring the system to the normal condition as soon as possible. However, it is essential to acknowledge that the actions of these protection schemes can potentially have adverse effects on the power system (Eremia & Shahidehpour, 2013). For instance, these protective actions may impact the system's stability (Eremia & Shahidehpour, 2013). Basically, initiating events cause high currents and low voltages in the power grid because of power system oscillations and voltage fluctuation. These changes in the currents and voltages may mislead the protection devices on other components (transmission lines and generators) and be treated as a fault. As a result, the stability margin of the system is reduced, and the remaining components are burdened with additional loads, potentially leading to further component failures and an accelerated cascade. According to (Eremia & Shahidehpour, 2013), protection schemes action accounts for about 70% of the U.S.-Canadian 2003 blackout. To be more specific, in this case, a significant number of the critical transmission lines tripped due to zone 3 (or zone 2) impedance relays while responding to overloads rather than faults on the protected component.

2.4.3 Cascading failures propagation, timeline, and stages

As discussed, the general mechanism behind the cascading failures can be divided into six stages, beginning with the pre-conditions and the initiating event that might trigger a successive chain of component failures leading to a blackout. Besides, as discussed in the previous section, after the occurrence of the initiating event and during the chain of cascading failures, power system stability issues might appear that affect the propagation and severity of cascading failures and blackouts and need to be addressed. In this regard, this section aims to investigate the generic underlying mechanism behind the propagation of cascading failures considering the dependency between the pre-conditions, initiating events, power system stability, and protection schemes.

A detailed discussion about mechanisms of blackout, including the five most critical types of phenomena behind system response during cascading failures, can be found in Annex II: Analysis of cascading failures.

Previous sections of this report have conducted a comprehensive investigation into the different stages of cascading failures and the mechanisms behind the propagation of these failures. In this section, a detailed timeline of cascading failures is presented, starting from the initiating event and leading up to a complete blackout and recovery. Figure 6 illustrates the transition between various operating conditions during cascading events. According to this figure, during the transitions between various states of a system, various events can occur, leading to changes in the system's operating conditions. These events stem from diverse sources and can have both positive and negative impacts on the system's security and reliability. Generally, events originate from three main sources: the system's initial response, control actions taken by operators, and incidents. The system's natural response primarily relates to the steady-state and dynamic behavior of power systems. Control measures encompass actions implemented by power system operators in response to other events, aiming to improve the system's state. Lastly, incidents involve accidental events within the system, such as disturbances or malfunctions. When the power system enters the alert or emergency stage, operators should take effective remedial actions to restore the system to normal conditions. If these measures are inadequate to mitigate the situation, the power system may face the risk of a blackout.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

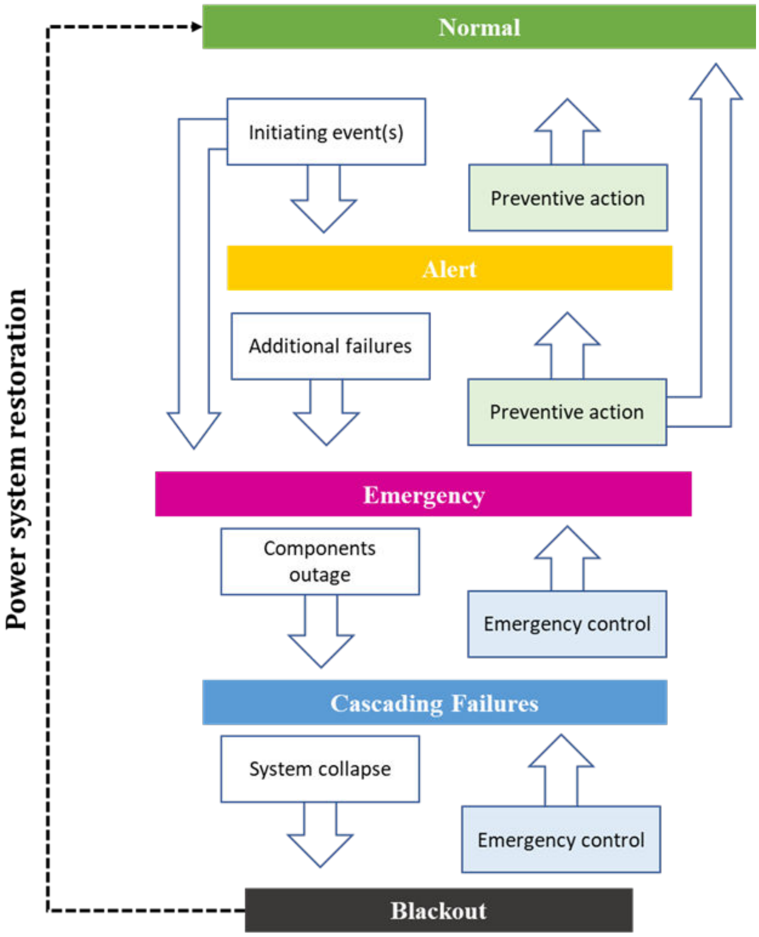


Figure 6. Main operational states in power system

Figure 7 provides a detailed illustration of the slow cascading events stage, representing a general scenario of the initial phase of cascading failures. It presents the timeline, system state, preventive and corrective actions, and the associated conditions in the sequence of events leading up to the point of no return. The dominant stability phenomena observed in this stage are long-term voltage and frequency stability, although sub-synchronous oscillations may also occur depending on the system's operating conditions. In terms of protection schemes, the most influential role in component outages is played by distance relays, particularly the zone 2 and 3 functionalities. Other protection relays, such as over and under voltages, can also result in tripping during this phase.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

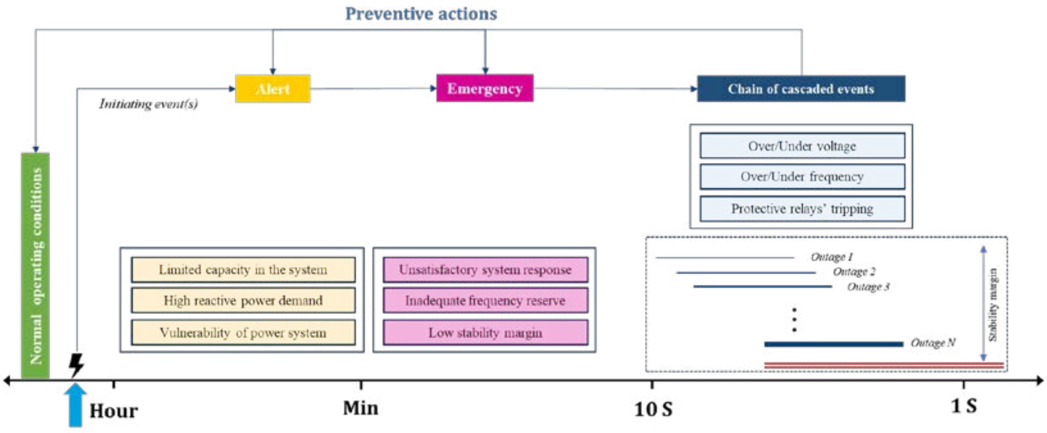

Preventive actions
Initiating event(s)
Alert
Emergency
Chain of cascaded events
Over/Under voltage
Over/Under frequency
Protective relays' tripping
Normal operating conditions
Limited capacity in the system
High reactive power demand
Vulnerability of power system
Unsatisfactory system response
Inadequate frequency reserve
Low stability margin
Outage 1
Outage 2
Outage 3
Outage N
Stability margin
Hour
Min
10 S
1 S

Figure 7. Timeline of slow cascading failures phase

2.4.3.1 Slow cascading failures

During the slow cascading events stage, the outage of each component alters the operating condition of the system, causing cascading effects. These effects manifest as operational problems, including overload, under voltage, and frequency fluctuation, propagating through the power grid, leading to further detrimental effects. Therefore, operators must take predefined remedial actions to mitigate these effects and prevent the propagation of failures. Estimating the available security margin before reaching the point of no return plays a vital role in implementing appropriate actions and preventing a blackout during this stage. However, it is important to note that each action taken by an operator can also have domino effects on the power system, potentially triggering a sequence of issues that push the system closer to the point of no return. For instance, after line outages, inefficient power flow dispatch by the operator may cause overload and voltage drop in another transmission line, leading to the tripping of additional lines in the system. Therefore, anticipating the system's response in this stage is critical for grid operators to mitigate cascading effects and prevent system collapse effectively.

The point of no return represents a significant turning point that distinguishes the slow and fast phases of cascading failures. In the first phase, the failure of one component propagates through the system, triggering additional domino effects. These cascading effects grow exponentially, resulting in severe issues for power system operation. As mentioned earlier, if operators cannot adequately alleviate these effects, the system enters a new phase in which cascading failures can lead to system collapse and a blackout.

2.4.3.2 Point of no return

During this slow phase, the system's response is relatively slow, providing operators enough time to respond and recover the power system. In contrast, the fast phase is characterized by rapid dynamics of the power system, significantly limiting the operator's reaction time.

As discussed earlier, the transition point between the slow and fast cascading stages is commonly referred to as the "**point of no return**." The point of no return represents a critical moment in the progression of cascading failures, where a large number of

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

components are tripped successively in a short time. Hence, it is almost impossible for the system to be recovered and restored. Understanding the point of no return is crucial for power system operators in managing cascading failures and mitigating the severity of blackouts. It helps determine the critical components or time that led to irreversible system instability and guides decision-making regarding system islanding or other remedial actions. By incorporating advanced monitoring, control, and predictive analytic techniques, operators can enhance their ability to identify the point of no return in a real-time or even anticipate its approach, enabling more effective response strategies and minimizing the consequences of cascading failures and blackouts.

2.4.3.3 Fast cascading failures

In the fast cascade phase, the system rapidly reacts to each disturbance, leading to several stability issues. Due to the vulnerability and fragility of the system in this phase, the inherent response of the system alone cannot maintain stability and mitigate these issues. Therefore, predefined protection schemes come into play to preserve the stability of components and the system. However, due to the critical operating condition of the power system, the protection system performance not only failed to preserve the system stability but can also exacerbate the situation, resulting in a rapid sequence of failures. This stage primarily involves the interaction between the fast system dynamics that drive instability and the protection system's efforts to maintain stability. These interactions are observed in various stability phenomena, including frequency stability. Short-term frequency stability represents a fast and global issue and constitutes a crucial aspect of the system's response during this phase. The significant mismatch between load and generation can cause huge frequency excursions. All running synchronous machines engage in frequency recovery. However, if the system lacks an adequate spinning reserve, the frequency drops dramatically, leading to the tripping of more generators due to frequency protection measures. In such circumstances, more outages cause further generation loss, leading to a faster frequency decrease and a repeating cycle of events. Given the rapid propagation of frequency deviations in the system, operators cannot rely solely on manual control to restore system conditions. Hence, implementing meticulous automated control actions is crucial to prevent a blackout during this stage. For example, load-shedding relays attempt to balance demand and generation by automatically shedding some loads in the system. Moreover, controlled islanding can suppress cascading failures and safeguard the power system against the risk of blackouts. Figure 8 presents a detailed timeline of the fast cascade phase, including protection actions and the building blocks of cascading failures.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

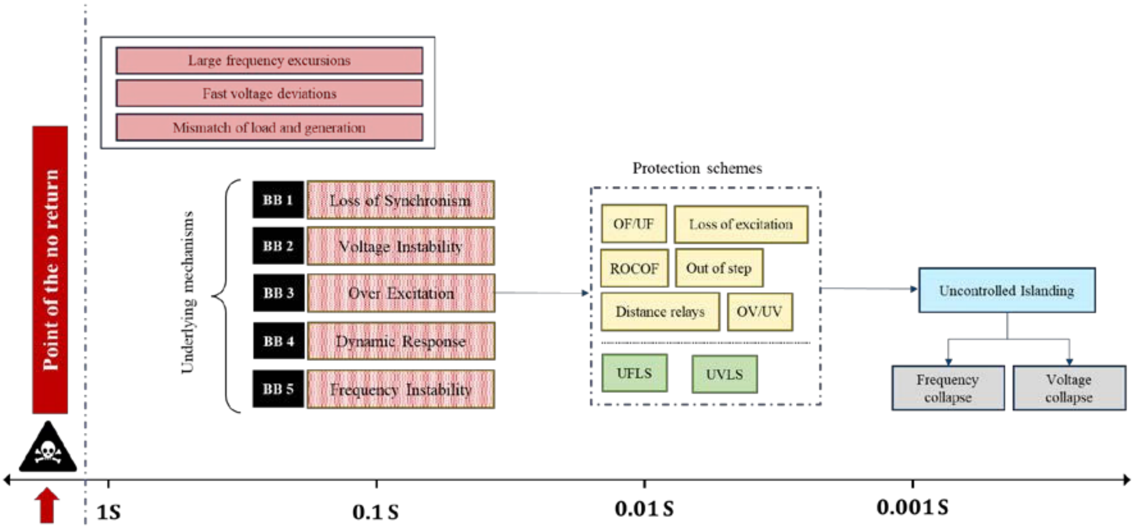


Figure 8. Timeline of fast cascading failures phase

2.5 Cascading failures accelerated by cyber-attacks

2.5.1 Overview of cyber-physical power systems and vulnerabilities

The increasing frequency and intensity of power outages in recent years have brought significant attention to the vulnerability and resilience of power systems. In response to these challenges, power systems have undergone a transformation into Cyber-Physical Systems (CPS) by integrating advanced Information Technology (IT) and Operational Technology (OT) networks. CPS enables the electric grids to have enhanced monitoring, communication, optimization, and control capabilities, delivering flexible, efficient, and reliable electricity to consumers. However, the interconnectivity and complexity of CPS also expose them to various vulnerabilities, including cyber threats and physical disruptions. To ensure the reliable and resilient operation of these systems, it is essential to understand cyber-physical power systems and their vulnerabilities (Paul et al., 2022).

2.5.1.1 Cyber-physical power systems

To comprehend the vulnerabilities of CPS, it is crucial to understand their architecture and key elements. CPS integrates advanced sensors, intelligent automation systems, and communication networks into power systems, with various definitions offered by different perspectives in literature. A common understanding of CPS is as complex automated systems comprising interdependent, multidimensional, and heterogeneous networks using collaborative computation, communication, and control technologies to provide efficient, reliable, secure, and resilient electricity.

Based on the Smart Grid Architecture Model (SGAM) National Institute of Standards and Technology (NIST) (Greer et al., 2014), CPS can be divided into five domains: markets, generation, transmission, distribution, and customers. These domains interact with each other to fulfill various power system applications, and each domain plays specific roles. The connection and interdependencies of these domains are crucial for a fully functioning CPS. As described in Figure 9, The market domain encompasses interactions with

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

external entities, including generation, transmission, distribution, and customers. Internally, there are communications among various functions such as market management, operations, wholesales, trading, ancillary operations, retailing, and distributed energy resource aggregation. Similarly, the customer domain has internal communication links among its components and also involves external communications and electrical exchanges with both the market and distribution domains. Within the transmission and distribution domains, there are intricate communication networks and electricity flows that operate within each respective domain.

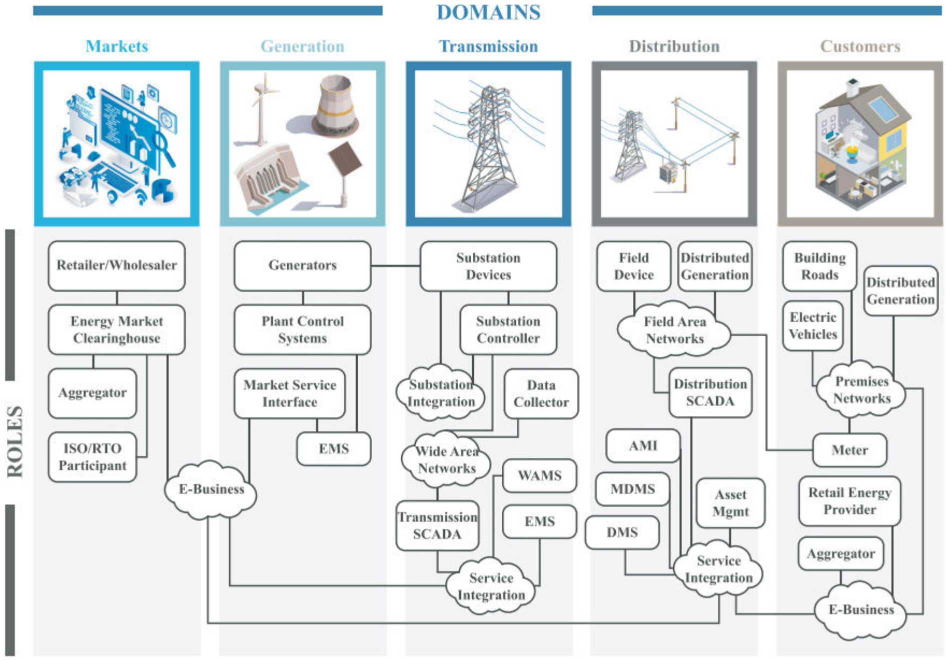


Figure 9. The architectural framework of the CPS consists of multiple domains (Paul et al., 2022)

2.5.1.2 Vulnerabilities in cyber-physical power systems

Vulnerability refers to the measure of a system's weakness concerning cascading events that may lead to outages, malfunctions, or failures (Baldick et al., 2009). Vulnerabilities in CPS can be classified into three types: cyber vulnerability, physical vulnerability, and cyber-physical vulnerability.

A. Cyber vulnerability

CPS relies on computer networks for control, and the integration of IT and OT has expanded the threat surfaces for attackers. Network vulnerabilities can arise from misconfigurations, poor administration, and lack of perimeter awareness (Stouffer et al., 2014). Communication protocols may lack authentication and encryption, leaving transmitted messages open to interception and manipulation (Chen et al., 2015). Heterogeneous devices connected to the system increase attack surfaces, and weak passwords and authentication in remote access points can lead to unauthorized intrusions.

B. Physical vulnerability

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Physical vulnerabilities in CPS involve damage to sensors, measurement devices, protection relays, transmission lines, towers, and transformers. Coordinated attacks on high-voltage transformers can cause widespread power outages with severe social and economic consequences (Parfomak, 2014).

C. Cyber-physical vulnerability

Cyber-physical vulnerability examines the correlation between cyber networks and physical systems in CPS. Coordinated attacks on cyber networks can amplify physical system damage. Physical failures can lead to cyber network malfunctions. The interdependence of cyber and physical elements makes CPS susceptible to cyber-physical threats and vulnerabilities (Vellaithurai et al., 2015).

2.5.1.3 Resilience in cyber-physical power systems

Resilience refers to a system's ability to anticipate, prepare for, adapt to changing conditions, withstand disruptions, and rapidly recover. Resilience in CPS can be categorized into cyber resilience, physical resilience, and cyber-physical resilience.

A. Cyber resilience

Cyber resilience emphasizes preventing cyber failures and managing cyber risks to maintain critical functions during cyber-attacks. A resilient communication network design can help prevent severe failures, and defense strategies against cyber-attacks and cyber network self-healing can aid in minimizing damage and facilitating recovery (Jacobs et al., 2018).

B. Physical resilience

Physical resilience focuses on a system's ability to absorb and recover from high-impact events (Staid, 2021). Short-term resilience involves dynamic resistance and adaptation during events, while long-term resilience relates to comprehensive system planning and infrastructure hardening.

C. Cyber-physical resilience

Cyber-physical resilience aims to respond to cyber-physical disturbances in real-time and mitigate major interruptions. It includes system identification, vulnerability analysis, and resilient operation to absorb disturbances and recover from failures.

2.5.2 Cyber-attacks on power systems

Modern power systems have undergone a significant transformation with the integration of advanced information and communication technologies, resulting in the emergence of CPS. These systems are critical infrastructures for modern society, enabling complex dual-directional information flow. However, this interconnectedness also makes CPS susceptible to cyber-attacks, which can lead to severe consequences, including power system blackouts. Recent incidents such as the Ukraine power outages in 2015 (Q. Guo et al., 2016) and Venezuela blackouts in 2019 (Vaz, 2020) serve as grim reminders of the potential havoc that cyber-attacks can wreak on power systems. Therefore, understanding and analyzing cyber-attack vectors on CPS is crucial for devising effective defense strategies.

In the following, a brief overview of various cyber-attack vectors prevalent in CPS is presented:

A. False Data Injection Attack (FDIA):

FDIA is a significant cyber-attack vector that targets power system state estimation. By injecting false data into meter measurements, the attacker can mislead the state estimator and cause undesirable outcomes in the power system (Liang et al., 2017).

B. Denial-of-Service (DoS) attack:

DoS attacks aim to disrupt the target server's ability to provide services properly. DoS attack is a destructive mode of attack that consumes the resources of a remote host or network until the system stops responding or crashes and the attacked computers or networks cannot provide normal services to the users.

C. Man-in-the-Middle (MITM) attack:

MITM attacks exploit the lack of authentication in a system, allowing attackers to intercept and manipulate message packets between two communication computers. Address Resolution Protocol (ARP) spoofing and Domain Name System (DNS) spoofing are cited as two common forms of MITM attacks, along with their potential impact on power systems.

D. Replay attack:

Replay attacks focus on intercepting a system's usage pattern to mislead the receiver. Replay attack is mainly used in the process of identity authentication and destroys the correctness of authentication (Zhao et al., 2016). The attacker sends a message packet that has been received by the target host to spoof the system.

E. Other attacks:

These include GPS Spoofing Attacks (GSA) targeting phasor measurement units, Load-Altering Attacks (LAA) against demand response programs, and Delay Attacks that disrupt communication channels.

2.5.3 Critical factors in cascading failures enabled by cyber-attacks

In this section, the crucial factors that contribute to cascading failures are explored, and the correlation between cyber-attacks and these critical factors also is investigated. Understanding this link is essential to comprehending how cyber-attacks can lead to cascading failures. Consequently, this insight will facilitate the development of effective measures to mitigate cyber-attacks and strengthen the defense against cascading failures.

In the following, a brief overview of major crucial factors in cascading failures is presented:

A. Mismatch of load and generation:

One of the most critical factors leading to cascading failures is the imbalance between demand and generation, which can result in several stability issues, notably a high rate of frequency changes. This vulnerability can be exploited through various attacks, such as FDIA, spoofing, and load-altering attacks.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

B. Reactive power reserve:

Reactive power plays a pivotal role in maintaining the voltage profile and preventing voltage collapse. When there is an insufficient supply of reactive power, it can lead to a significant voltage drop, rendering the system more vulnerable to other failures. Exploiting this critical factor is possible through various attacks, including FDIA, spoofing, and DoS attacks.

C. Spinning reserve:

System inertia, also known as spinning reserve, plays a crucial role in the dynamic response of the system to various disturbances. A system with low inertia is highly susceptible to losing stability when confronted with large faults. This critical factor can be exploited through various attacks, including FDIA and spoofing.

D. System malfunction

Misconfigured relays, circuit breaker malfunctions, and incorrect control actions can significantly jeopardize system stability and trigger cascading failures, even under completely secure operating conditions. This critical factor leaves the system vulnerable to exploitation through all types of attacks, including FDIA, DoS, and spoofing.

2.6 Attacks on electricity demand

2.6.1 Load altering attacks and cascading failures

In the previous section, cyber-physical system vulnerabilities and their associated critical factors are discussed. The simulation results section serves as a crucial stage in this investigation into the link between critical factors in cascading failures and the potential role of cyber-attacks in exploiting them. By exploring this connection, this study aims to shed light on how cyber-attacks can be utilized to initiate or accelerate cascading failures within power systems. In this study, the load-altering attacks on Electric Vehicle Charging Stations (EVCS) are investigated.

Load-altering attacks can be carried out using smart grid load-management capabilities, such as demand-side management and home automation, or through specific loads, such as electric vehicles. The aim of these attacks is to manipulate the demand for electricity in a way that causes the power system to become overloaded or underutilized, leading to disruptions in service. The potential consequences of these disruptions range from local blackouts to widespread power outages that affect entire regions or even countries. The conducted simulations cover, in detail, the following subjects:

- Effects of load-altering attacks on the IEEE 39-bus system by analyzing the dynamic system's behavior under different attack scenarios, including decreasing, increasing, and combined load-altering attacks.
- The minimum required load to be changed to cause cascading failures and blackouts is derived through a brute force algorithm. The critical levels of increasing/decreasing the load that can trigger cascading failures are identified.

The findings of this study are that in normal and stable operating conditions, manipulating at least 36% of the total load (increasing or decreasing) is necessary to cause significant cascading failures and lead to a blackout. Detailed simulation results can be found in Annex III: Simulation results.

2.6.2 MaDIoT attacks

With the growing deployment of IoT devices at the consumer level, cyber-attacks may not only target the SCADA systems of the utilities but also try to exploit the weaknesses of these devices. IoT devices usually have a lower level of security and, when massively compromised. This weak level of security can be used to decrease the security margins of the power system, cause load shedding, or a cascading effect that ends up in a wide-area blackout (Dabrowski et al., 2017; Soltan et al., 2018). In addition to having more surface attack consumer level, it is also more vulnerable than SCADA systems. Moreover, high-wattage devices, such as EV charging points, are not continuously monitored by the system operator (Acharya et al., 2020).

In (Mohsenian-Rad & Leon-Garcia, 2011), the concept of an internet-based load-altering attack was defined, identifying direct and indirect loads that could be potentially compromised. MaDIoT attack was introduced by (Soltan et al., 2018) as an attack that disrupts the normal operation of the power grid by altering the power demand using IoT devices to which the attacker has access. Authors (Soltan et al., 2018) studied these attacks on the Polish grid model, managing to cause local outages and large blackouts in the grid. However,(Huang et al., 2019) suggest the possibility that the Polish grid model under analysis was not N-1 secure, which would lead to an overestimation of the impact of the attacks.

(Huang et al., 2019) shows that causing a wide area blackout in a large North American regional system using evenly distributed MaDIoT attacks is extremely difficult; even if the grid is in a vulnerable state prior to the attack, such attacks would only cause partial blackouts due to the partial disconnection of the loads (UFLS protection), and generators (ROCOF protection). The system would quickly recover its stability after this.

In (Shekari et al., 2022), authors studied MaDIoT attacks on the IEEE 39-Bus system, assuming the attacker had advanced knowledge about the system; this would allow them to perform more advanced attacks targeting the most vulnerable nodes in the power system. Results (Shekari et al., 2022) show that these attacks present success rates between 67 and 91% in causing widespread blackouts; however, the likelihood of an attacker with the required system knowledge and resources is estimated to be low.

To study and compare the impact of MaDIoT attacks on power systems with different characteristics, simulations using DIgSILENT PowerFactory have been performed within task T2.2 of the project. Two test systems were considered: the IEEE 39-Bus system (New England system) and PST-16 Benchmark system (simplified European-like model with three areas A, B, and C). Details on these two models and the scenarios considered can be seen in Annex IV: Modelling details for MaDIoT attacks. The following section presents the main results obtained when simulating MaDIoT attacks and conclusions.

2.6.2.1 Simulation results

Figure 10 shows the success ratio (number of successful attacks / total number of attacks) of the MaDIoT attacks in the scenarios considered (see Annex IV: Modelling details for MaDIoT attacks) so that the different impact of the attacks on the two systems can be better appreciated and compared.

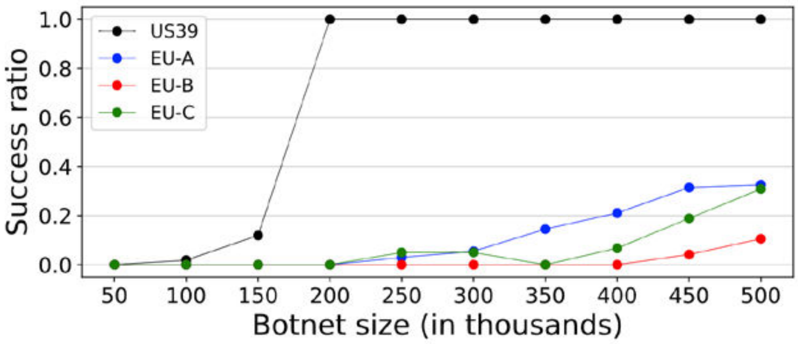


Figure 10. The success ratio for the scenarios in Table 10 when increasing the size of the botnet.

In the US39 scenario, all the attacks that compromised more than 150k bots were successful. When increasing the attack from 150k to 200k, the change in the success ratio is significant, going from 10% to 100%. This means that, under the conditions assumed, it makes no difference if the buses attacked are close between them when compromising more than 150k bots. In other words, the attack will always cause the disconnection of loads or generation. Considering this, the attacker does not need advanced knowledge of the grid. Nevertheless, by carrying out its attack during the peak demand hour, the probability of success could be high in this scenario.

On the other hand, MaDIoT attacks start being successful in the EU-A and EU-C scenarios when compromising >200k bots and, in the EU-B scenario, for botnets larger than 400k. While EU-A and EU-C have a similar success ratio for a botnet of 500k bots (~30%), the EU-B scenario still presents a significantly smaller maximum success ratio (~10%). As shown in Figure 54, areas A and C present the highest gap between generation capacity and demand: area A has more generation than demand, while C depends on power imports from outside the area.

Therefore, the required number of bots to have a successful attack is lower in the New England system than in the PST-16, as it is also a smaller system.

Despite the differences in the success ratios for the New England and the PST-16 grid models, the probability of success is not tantamount to the impact degree (number of loads and/or generators disconnected). To illustrate this, two cases with a high impact in each model (one case per model) are shown in Figure 11 and Figure 13 and discussed below.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

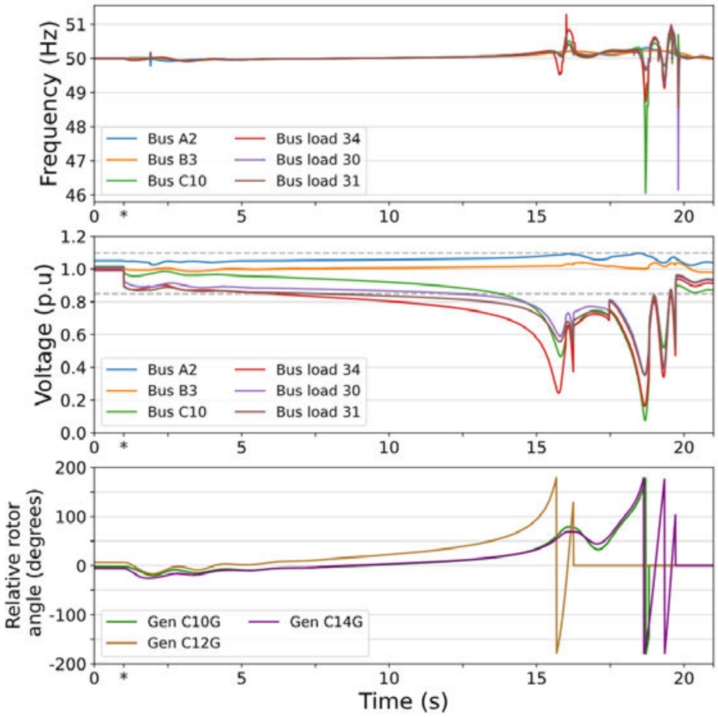


Figure 11. Frequency, voltages, and relative rotor angle of generators when attacking 500k bots in loads 30, 31, and 34 in the PST-16 system (EU-C scenario with high impact)

Figure 11 shows the frequency (Hz), voltage (p.u), and relative rotor angle of generators (with respect to the reference generator) when 500k bots are attacked in loads 30, 31, and 34 in the PST-16 system. The time of the attack (t=1s) is displayed on the x-axis as '*.' For the frequency and voltages, only six buses are displayed, including the ones attacked. As for the relative rotor angle, only three generators from area C are shown.

As shown in Figure 11, the attack significantly destabilizes the system. Figure 12 shows a zoom on the frequency and the relative rotor angle during the first 10 seconds of this case. In the frequency domain, the attack initially has a small impact that is only appreciated during a few seconds; there is a slight oscillation between areas, but the system manages to limit frequency variations and is apparently stable. However, when reaching t=15s, the frequency in area C diverges from the other two areas. The frequency of bus C10, which has generation connected, drops suddenly to 46 Hz at around t=18.5s. These frequency variations about 12 seconds after the attack are explained by the loss of rotor angle stability in the system.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

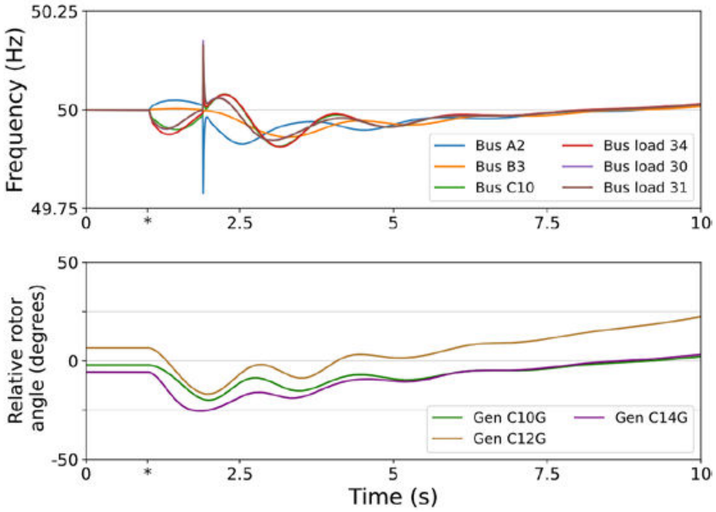


Figure 12. Zoom on the frequency and relative rotor angle for the first 10 seconds. EU-C scenario with high impact

The middle plot included in Figure 11 shows the immediate high impact that the attack has on the voltages of area C. Before the attack, this system was already operating under what could be considered peak-demand conditions, where area C depends on the power imports from areas A and B.

The voltages of the nodes attacked significantly decrease to just above the limit configured for the actuation of the under-voltage protections. However, due to the increase in demand caused by the attack, the system loses rotor angle stability and goes into a voltage collapse. The bottom plot of Figure 11 shows that the rotor angles in generators of area C start diverging with respect to the reference generator after some initial oscillations. Therefore, the system first experiences a rotor angle stability problem that leads to a voltage collapse.

Since voltages are below 0.85 p.u for more than 10s (Figure 11), under-voltage protections start actuating, disconnecting loads from the system. The actuation of these protections, together with the UFLS and OFGR protections in the frequency domain, are one of the main causes for the oscillations in the 15-20s interval. After the actuation of the protections, the system seems to recover by t=20s but with rather low voltage levels (e.g., at Bus C10). By that time, the OFGR scheme has disconnected around 2.9GW of generation from the system. However, the impact could be different if further protection features were implemented (e.g., distance protection with/without out-of-step protection, etc.). In this case, despite facing an increase in the demand because of the attack, the system ends up with around 3GW less demand than before the attack (~20% decrease) due to load shedding (UFLS and under-voltage protections). That is, not only the equivalent to the extraordinary demand caused by the attack had to be disconnected from the system, but that more loads had to be shed for the system to recover.

However, the effect of MaDIoT attacks may not be the same in other power systems. Figure 13 shows the frequency and voltages when attacking 500k bots in loads 12, 16, and 28 in the New England system (i.e., IEEE 39-Bus model).

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

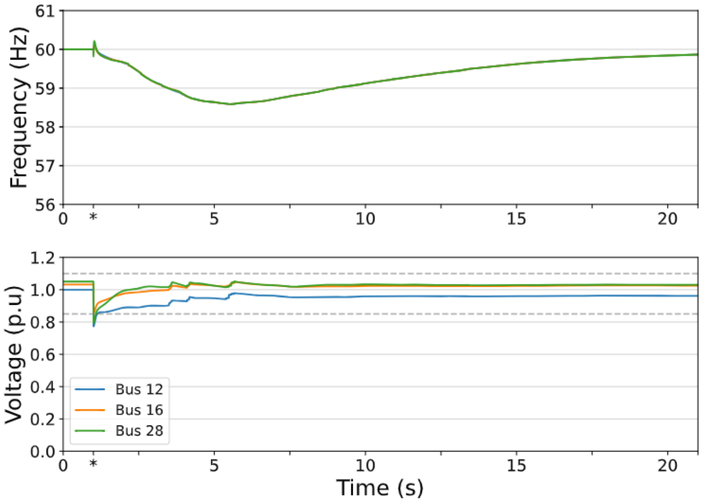


Figure 13. Frequency and voltages when attacking 500k bots in loads 12, 16, and 28 in the New England system. US39 scenario with high impact.

In this case, the immediate impact of the attack on the frequency and voltages of the system is significant. It can be observed that the frequency drops by 1Hz in approximately two seconds. Below 59 Hz, the UFLS scheme starts actuating, as described in Table 9 in Annex IV: Modelling details for MaDIoT attacks . This softens the drop in frequency; only when it reaches ~58.6Hz, the system starts increasing the frequency. However, the recovery is slow. In this case, the system manages to keep all voltages within limits, so the only protections actuating are the UFLS protections. These protections shed about 1.1 GW of loads along the system. Nevertheless, despite shedding loads, the demand for the system increases to 76 MW with respect to before the attack (~1.2% increase). This means that practically, the amount of demand disconnected is equivalent to the demand increase provoked by the MaDIoT attack. However, legitimate loads are also affected by this load shedding, as UFLS protections make no distinction. Compared to the EU-C case previously analyzed, the relative impact is smaller, as the system keeps its stability.

Although any attack compromising any three buses in the New England system may be successful, its impact could be relatively low, equivalent to the magnitude of the attack. On the other hand, causing instability in the PST-16 system is more complex as it is larger and has more resources to confront the attack; however, as discussed, a successful attack can significantly destabilize the system, causing the partial disconnection of loads and generation.

Therefore, the results obtained in T2.2 show the different types of impact that MaDIoT attacks have on grids with different characteristics. A higher success ratio of MaDIoT attacks does not necessarily mean a higher impact on the system. In the case presented for the PST-16 system, the attack causes rotor angle instability in area C and has an impact on voltages, whereas, for the New England system, the main impact was on the frequency, motivated by the high inertia of the generation in the model.

3 Actions to increase power system resilience

As we electrify all aspects of our lives, the modern society relies on electrical power. The current global economy requires electricity to be even more accessible, affordable, and continuously available. For this reason, any disruption to the energy supply chain will lead to catastrophic economic impacts. Power outages can trigger accidents and cause financial losses. To avoid these types of disruptions, actions to increase power system resilience should be undertaken. This section describes the approaches for resilience action identification aimed at reducing economic losses derived from disruptions at the physical and cyber layers. The actions are divided mainly into resilience measures implemented at the physical layer and cyber layer.

3.1 Physical layer

3.1.1 Approach to the identification of resilience actions

A report from Climate Central (Climate Central, 2022) has highlighted that 83% of major power outages between 2000 and 2021 were attributed to extreme weather. Also, the experiences of the electricity industry in the last decade highlighted the vulnerability of the sector to extreme events. The traditional approaches to extreme events were focused on reliability, security, restoration, and emergency planning. Based on present and past events, energy suppliers and public authorities should invest more in EPES resiliency to contrast natural events' impacts. In fact, in traditional approaches, the prevention aspects and recovery phase after an event are not considered. All these aspects are included in the risk and resilience assessment of EPES.

The Risk Assessment (RA) methodology considers three main phases. The first phase is before the event through the study of the hazard probability of occurrence, economic exposure, and structural characteristics of the assets. The second phase occurred during the event by calculating the vulnerability and the consequent capacity or functionality loss for the specific asset affected by a specific hazard having a specific intensity measure. And the phase after the event is finally studied based on structural losses, service interruptions, and exposed goods. The RA methodology will be realized within the eFORT project through the dynamic risk assessment tool for EPES. In this way, it is possible to identify specific resilience mitigation actions for each phase of the timeline considered in RA before, during, and after the event occurrence.

The resilience actions identification will be done based on the results of previous work performed in the project (Brasinika, 2023). For the definition of resilience, actions will be considered in the following aspects: asset categories and threats characterization. The RA was performed through a simple model and a detailed quantitative dynamic risk assessment. Prior to the detailed definition of the inputs needed for the identification of the mitigation actions, the EPES asset characterization and threats identification are reported. A summary of the EPES asset characterization is described in Annex I: EPES asset characterization.

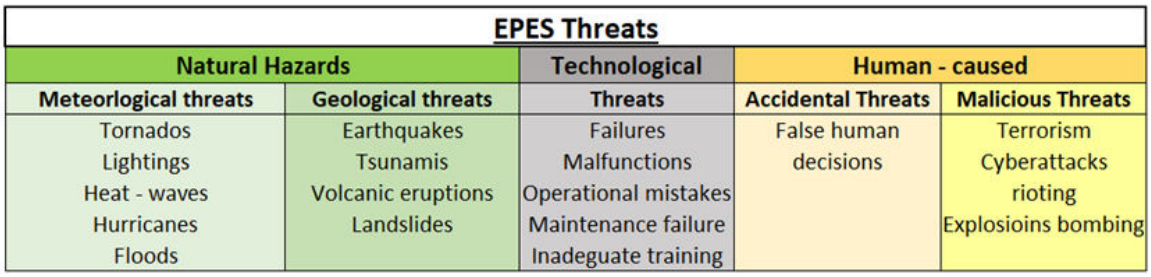
This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

3.1.2 EPES vulnerabilities and impacts

In this section, the inputs needed for the resilience mitigation actions are described. The first aspect to be considered is the classification of the EPES and list of possible threats that can cause interruption in energy supply. Once these aspects are clear, vulnerabilities and induced losses are interpreted to identify and assign one or more mitigation actions to be performed on an electric power system and increase its resiliency against natural threats.

An important aspect of the resilience mitigation action definition is the classification of EPES threats. The main threats that can impact electrical power sectors are typically natural, technological, or human-caused threats.

Natural threats can be caused by environmental, meteorological, and natural phenomena such as tornados, lighting, heat waves, hurricanes, or geological hazards, such as earthquakes, tsunamis, volcanic eruptions, etc. Technological threats may include equipment failures or malfunctions, operational mistakes, maintenance failure, or inadequate training, which can also be included in human-caused threats. Human – caused threats can be divided into accidental or malicious based on human intentionality. Accidental actions are generally associated with human decisions. Meanwhile, malicious actions are terrorism, cyber-attacks, rioting, explosions bombing, etc.



EPES Threats				
Natural Hazards		Technological	Human - caused	
Meteorlogical threats	Geological threats	Threats	Accidental Threats	Malicious Threats
Tornados	Earthquakes	Failures	False human decisions	Terrorism
Lightings	Tsunamis	Malfunctions		Cyberattacks
Heat - waves	Volcanic eruptions	Operational mistakes		rioting
Hurricanes	Landslides	Maintenance failure		Explosioins bombing
Floods		Inadeguate training		

Figure 14. Threats classification (Brasinika, 2023)

Possible impacts of these threats can be fuel supply shortages, physical infrastructure damage, shifts in energy demand, and disruption of electricity supply to the end-users.

The EPES vulnerability can be carried out through both qualitative and quantitative assessments, combining the likelihood of a threat occurrence and structural characteristics of EPES assets. The threat likelihood occurrence negatively affects the vulnerability of an EPES asset due to the asset location, where the probability of occurrence of natural hazards is high. Notably, the structural characteristics of an EPES asset also play a role in determining its vulnerability to potential threats. As per sector knowledge, the age and maintenance conditions of an asset affect its hazard-proneness. This can be described with a fragility-curve reduction model, as shown in Figure 15. Such a model can provide quantitative measures to compile a risk value associated with an asset.

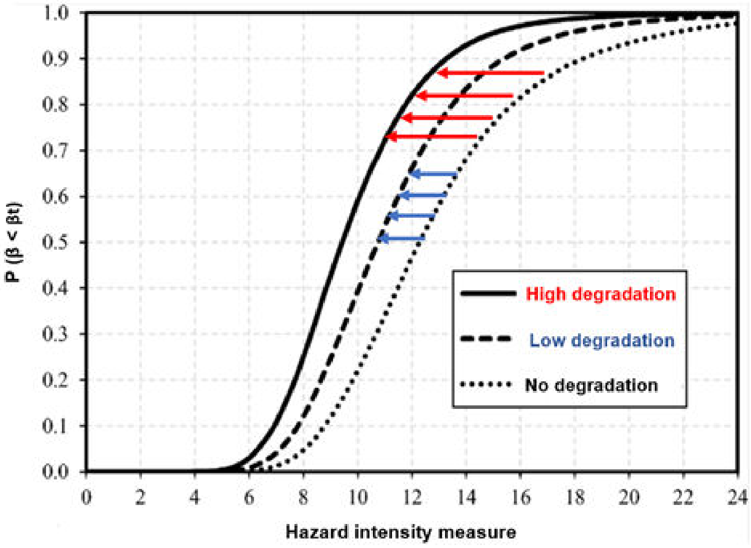


Figure 15. Fragility curve reduction

In both assessments, qualitative and quantitative, it is possible to estimate the level of damage that each threat may adversely cause on EPES assets, determining disruption of services, equipment damages, and the impact on employees or potential residents' health.

3.1.2.1 Input from dynamic risk assessment

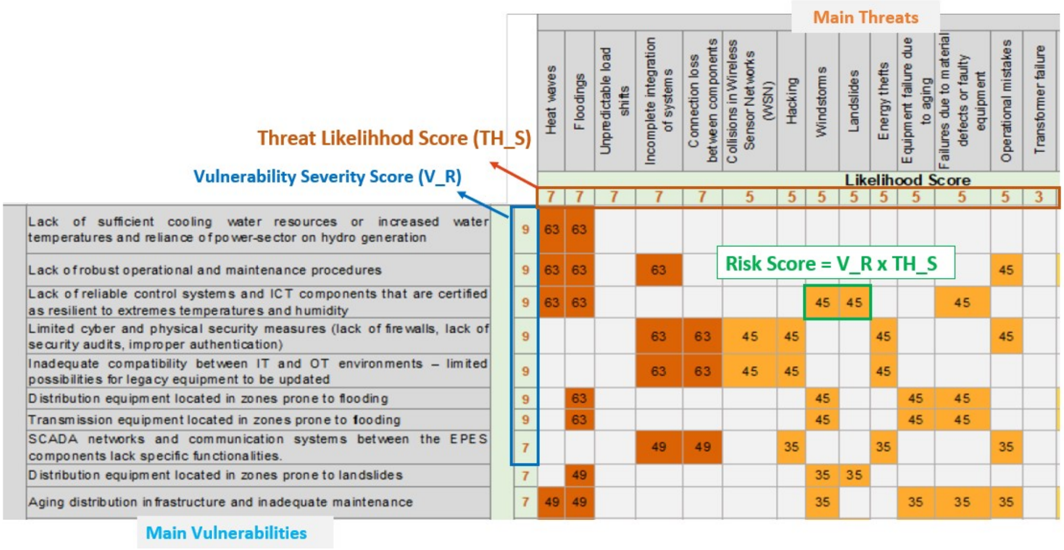
For the definition and prioritization process of the resilience mitigation actions, a key step is risk assessment. RA is a method to determine the nature and extent of risk by also integrating the likelihood of events. There are several approaches for RA. Here, for the RA of energy sector security, the framework proposed by ISO 31010 (ISO/TC 262 Risk management, 2019) and followed by the Joint Research Centre has been considered.

RA can be performed following two different levels, a simplified model and a detailed risk assessment. Typically, the first method can be classified as a qualitative method; meanwhile, the second method is a quantitative method.

The main goal was to prioritize the various risks related to the identified threats. A risk scoring process has been adopted combining the likelihood of a threat to occur, determined by the Threat Indicator, and the severity of the consequence of the potential vulnerabilities, indicated by the Vulnerability Severity Indicator.

The first step was to the correlation between threats and vulnerabilities by forming a matrix, as not all threats directly influence each vulnerability. Then, a Risk Matrix highlighting the relationships between threats and vulnerabilities was determined by multiplying the threat indicator by the vulnerability indicator.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.



Main Threats

Threat Likelihood Score (TH_S)

Vulnerability Severity Score (V_R)

Risk Score = V_R x TH_S

Main Vulnerabilities

Main Vulnerabilities	V_R	Heat waves	Floodings	Unpredictable load shifts	Incomplete integration of systems	Connection loss between components	Collisions in Wireless Sensor Networks (WSN)	Hacking	Windstorms	Landslides	Energy thefts	Equipment failure due to aging	Failures due to material defects or faulty equipment	Operational mistakes	Transformer failure
Likelihood Score		7	7	7	7	7	5	5	5	5	5	5	5	5	3
Lack of sufficient cooling water resources or increased water temperatures and reliance of power-sector on hydro generation	9	63	63												
Lack of robust operational and maintenance procedures	9	63	63		63									45	
Lack of reliable control systems and ICT components that are certified as resilient to extremes temperatures and humidity	9	63	63						45	45			45		
Limited cyber and physical security measures (lack of firewalls, lack of security audits, improper authentication)	9				63	63	45	45			45			45	
Inadequate compatibility between IT and OT environments – limited possibilities for legacy equipment to be updated	9				63	63	45	45			45				
Distribution equipment located in zones prone to flooding	9		63						45			45	45		
Transmission equipment located in zones prone to fooding	9		63						45			45	45		
SCADA networks and communication systems between the EPES components lack specific functionalities.	7				49	49		35			35			35	
Distribution equipment located in zones prone to landslides	7		49						35	35					
Aging distribution infrastructure and inadequate maintenance	7	49	49						35			35	35	35	

Figure 16. Simplified risk assessment (Brasinika, 2023)

In this first RA of the simple model, the exposure component does not appear in the risk score as has been involved in the vulnerability severity scoring. In general, RA is done by analyzing the potential frequency of hazard events and evaluating conditions of exposure and vulnerability that together could potentially harm exposed people, assets, and the environment. In fact, the three main components of the RA are hazard, vulnerability, and exposure (typically in economic terms). The hazard defines the hazard probability of occurrence, vulnerability defines the structure behavior against a specific hazard, and impact defines the value of the exposure.

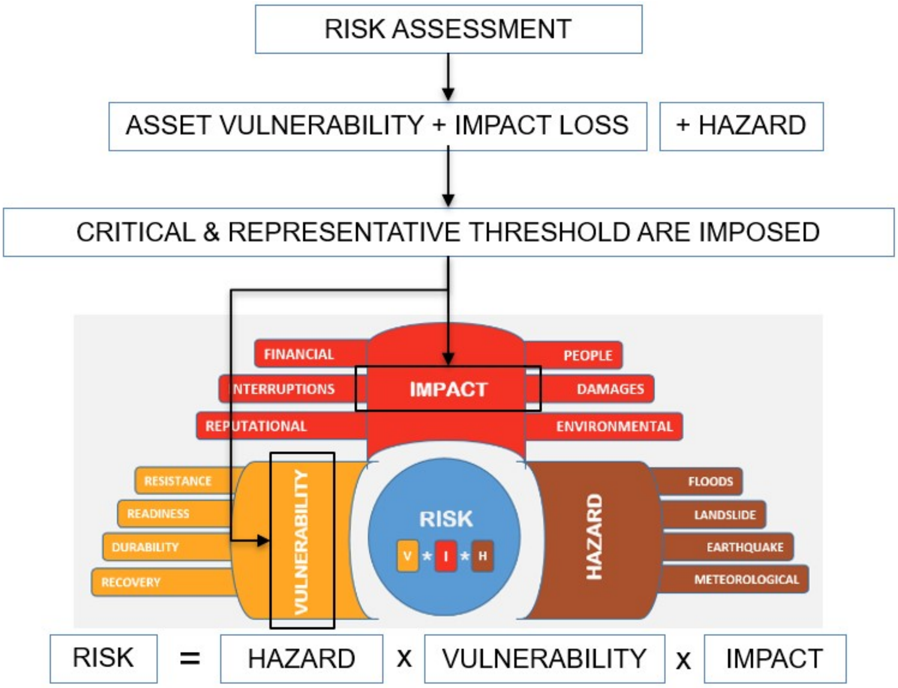


Figure 17. Dynamic risk assessment framework

Once the vulnerability is determined and probability of having the associated possible impacts is estimated, it is possible to determine the economic losses associated with those impacts. Thus, the service disruption determines the indirect losses derived from the interruption of service, equipment damages determine the direct losses, and impacts on people's health determine the economic losses deriving from people's injuries and deaths, also known as Death Losses.

The framework consists of these main steps:

I. EPES asset characterization and hazard characterization

II. Simple risk assessment

  a. Vulnerability scoring

  b. Hazard scoring

III. Quantitative risk assessment – dynamic risk assessment

IV. Resilience actions identification based on the outputs of RA evaluations

To identify the resilience mitigation actions, at least one of the RA analyses is needed. This depends on the budget and data availability. The best practice would be that the simple method should be used as a screening process to prioritize main EPES assets and threats. Then, starting from these worst-case scenarios, the quantitative RA method should be applied to assess and define possible economic impacts through detailed analyses. In fact, quantitative RA is a more robust methodology and requires detailed inputs and computational effort. The main workflow is described in the following framework.

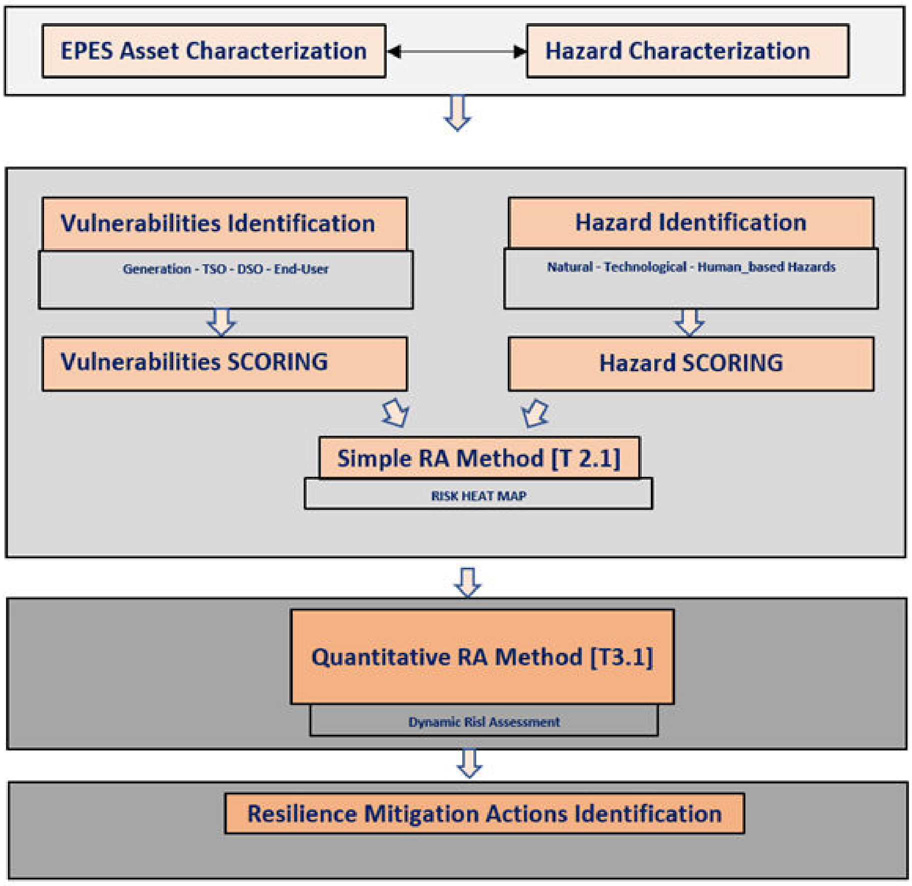

EPES Asset Characterization
Hazard Characterization
Vulnerabilities Identification
Generation - TSO - DSO - End-User
Hazard Identification
Natural - Technological - Human_based Hazards
Vulnerabilities SCORING
Hazard SCORING
Simple RA Method [T 2.1]
RISK HEAT MAP
Quantitative RA Method [T3.1]
Dynamic Risl Assessment
Resilience Mitigation Actions Identification

Figure 18. Main Framework for the Resilience Mitigation Actions Identification

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

3.1.3 Resilience actions

A resilient power system is one that has the capacity to withstand disturbances and continue to deliver energy to customers. The EPES service is closely related to customers, so resilience can be described as: "*the ability to withstand and reduce the magnitude and/or duration of disruptive events, which includes the capability to anticipate, absorb, adapt to, and/or rapidly recover from such an event*."

The reason that power systems are particularly vulnerable to extreme weather events is that they are mainly designed and optimized for normal weather conditions and are not equipped to handle less common extreme weather events.

Another aspect is that disasters that lead to shocks and stresses are often connected, making the risk two-fold. For example, higher temperatures due to climate changes result in higher power demands, therefore increasing the load on the power system.

In a more general context, the National Advisory Council (NIAC) has listed four attributes of a resilient system, which are *robustness, redundancy, resourcefulness, and rapidity*. Also, (Cimellaro et al., 2010) have identified these 4 properties in various resilient systems, typically named the four Rs.

- **Robustness**: is the strength or ability of elements, systems, and other measurements of analysis to withstand a given level of stress or demand without degradation or loss of function.
- **Redundancy**: is the capacity to satisfy functional requirements in the event of disruption, degradation, or loss of functionality.
- **Rapidity**: is the capacity to meet priorities and achieve goals in a timely manner in order to contain losses, recover functionality and avoid future disruption.
- **Resourcefulness**: is the capacity to identify problems, establish priorities, and mobilize alternative external resources such as information, capital, technology, and manpower.

Mitigation actions are divided into preventive, corrective, and restorative measures, which shall be done respectively before, during, and after the event. The main goal of these three types of mitigation actions is to increase and improve EPES resiliency, as shown in Figure 19.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

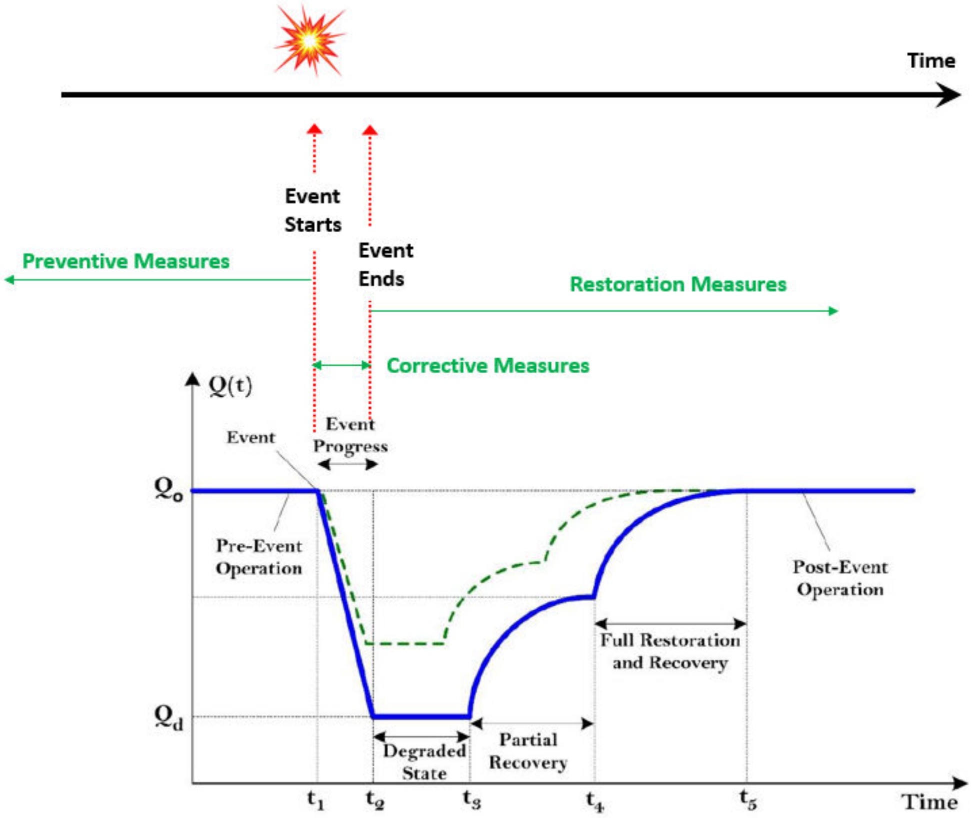


Figure 19. Mitigation actions identification during an event occurrence

The four attributes of a resilient system are strictly connected to the principal scheme of resilience reported in the DoA: anticipate, absorb the shock, adapt to and recover from attacks/natural events.

Preventive measures

All threats are characterized by non-uniform probability occurrences in the territory. For this reason, crucial systems for the electrical network (data centers, control rooms) shall be implemented in low-risk areas. Technical choices can be driven by the knowledge of the threats with a high probability of occurrence. Underground cables can be used instead of overhead lines in areas exposed to thunderstorms.

- Risk mask in the territory.
- Implementation of important systems in low-risk areas.
- Technical choices to prevent faults.

Redundancy is always a good practice against all threats. Systems with more parallel lines and meshed networks are more resilient.

- Parallel lines.
- Meshed grid.

Systems with highly distributed resources mitigate the impact of an event. The loss of a relevant generation or consumption unit would be more difficult to deal with.

- Distributed generation.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Preventive maintenance is clearly a key measure to reduce fault occurrences. Both maintenance of electric components and of the environment are needed. The management of trees close to overhead lines can prevent the fault from the fall of trees because of thunderstorms.

- Maintenance of electric components.
- Maintenance of the surrounding environment.

High-priority systems such as hospitals should have available emergency generators (Uninterruptible Power Supply – UPS) or storage systems.

- Emergency generators.

It is mandatory that the power system is designed with a protection system and a measurement system.

- Protection system.
- Measurement system.

Regulation services represent the tool of the TSO to change the power injections guaranteeing the power system stability and reliability. They are applied to meet the balance between power generation and consumption both in normal operating conditions and in fault emergency conditions. In the first case, regulation services are foreseen by the daily electricity market and can be intended as a preventive action to avoid blackouts.

- Regulation services.

Corrective measures

Given the danger of natural threats and the fast dynamic of electrical faults, there are low chances of acting during the event.

The protection system opens the circuit when a fault occurs to isolate it and protect the safe portion of the network.

- Protection system.

Regulation services represent the tool of the TSO to change the power injections guaranteeing the power system stability and reliability. They are applied to meet the balance between power generation and consumption both in normal operating conditions and in fault emergency conditions. In the second case, when a fault event occurs in a portion of the network, some generation and load units can be requested to change their power profile output or demand to keep the rest of the network properly working, even if in emergency conditions. In this case, the service is a corrective action as it takes place after the event, but before the system restoration, so when the emergency is still ongoing. A clear example of regulation service is the curtailment of Renewable Energy Sources (RESs) as they usually operate at maximum power and sometimes have to reduce the power production depending on the network needs.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

- Regulation services.

Restorative measures

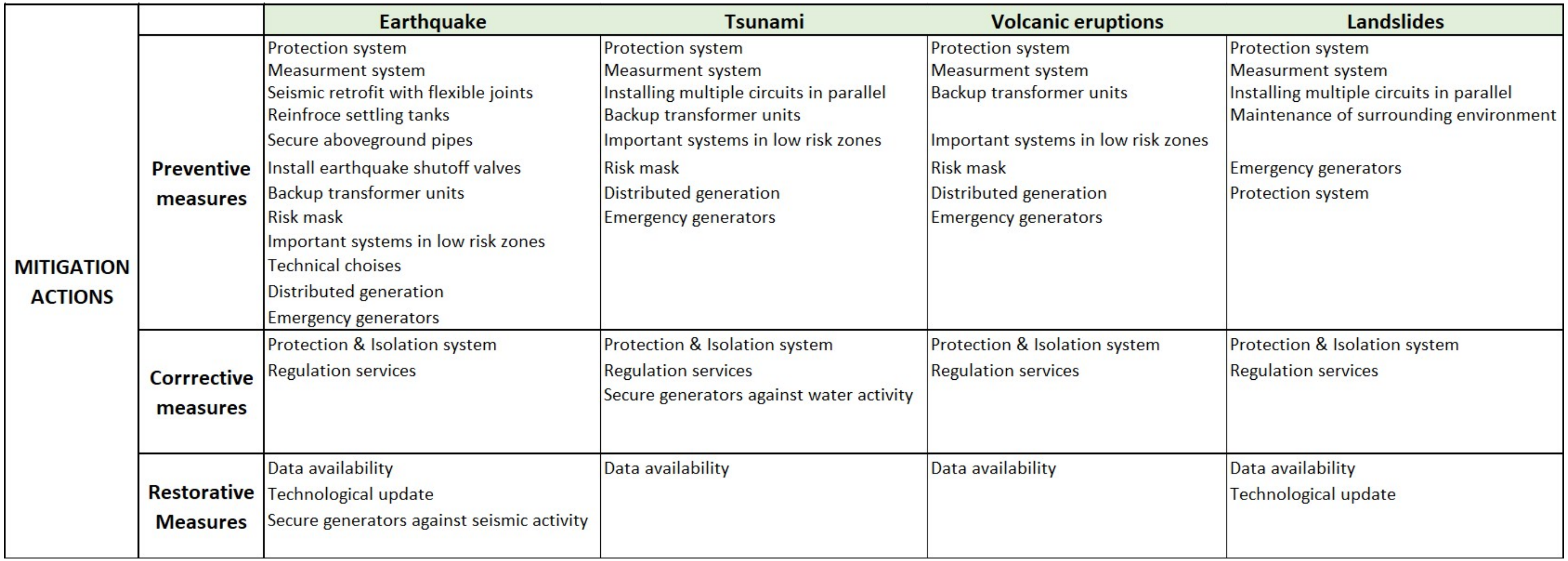
After faults, there is the possibility of redesigning the power system to increase its resiliency for the next event. Also, a fast recovery of the service is requested to minimize losses.

Access to data and measures can support the identification of the fault and speed up the restoration of the electrical system. In this phase, there is also the chance to update the system with new technologies.

- Data availability.
- Technological update during restoration.

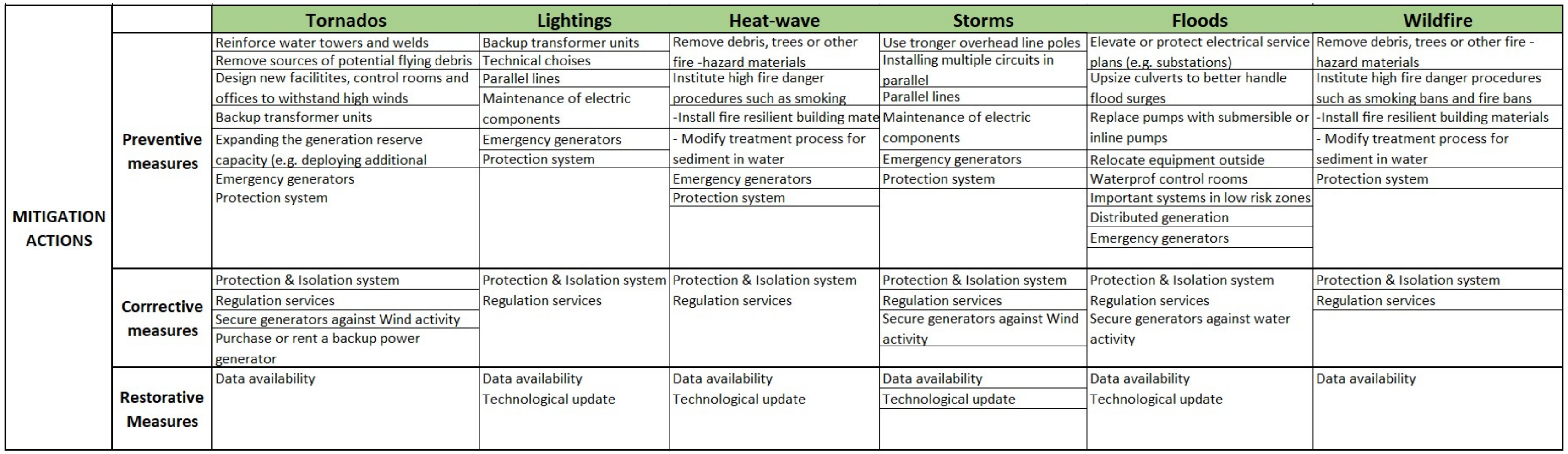
Starting from the previous general mitigation actions definition and other specific mitigation actions, a correlation between those mitigation actions and possible threats occurrence has been defined. Considering only the generic mitigation actions, a correlation with the possible threats and impacted EPES components has been defined, as shown in Figure 21.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.



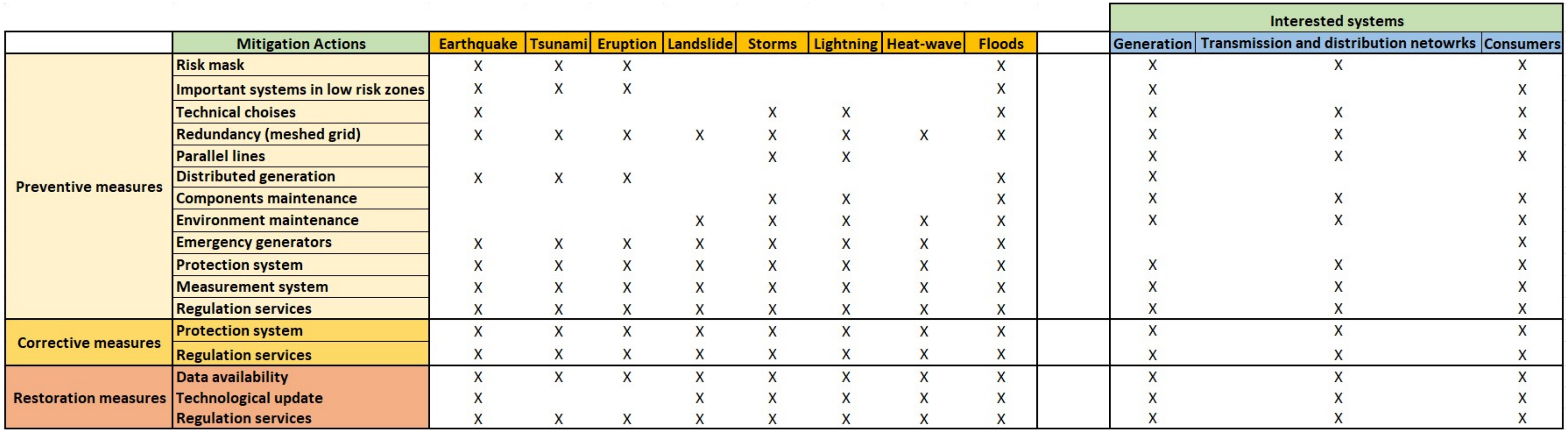
		Earthquake	Tsunami	Volcanic eruptions	Landslides
MITIGATION ACTIONS	Preventive measures	Protection system Measurment system Seismic retrofit with flexible joints Reinfroce settling tanks Secure aboveground pipes Install earthquake shutoff valves Backup transformer units Risk mask Important systems in low risk zones Technical choises Distributed generation Emergency generators	Protection system Measurment system Installing multiple circuits in parallel Backup transformer units Important systems in low risk zones Risk mask Distributed generation Emergency generators	Protection system Measurment system Backup transformer units Important systems in low risk zones Risk mask Distributed generation Emergency generators	Protection system Measurment system Installing multiple circuits in parallel Maintenance of surrounding environment Emergency generators Protection system
	Corrrective measures	Protection & Isolation system Regulation services	Protection & Isolation system Regulation services Secure generators against water activity	Protection & Isolation system Regulation services	Protection & Isolation system Regulation services
	Restorative Measures	Data availability Technological update Secure generators against seismic activity	Data availability	Data availability	Data availability Technological update

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.



		Tornados	Lightings	Heat-wave	Storms	Floods	Wildfire
MITIGATION ACTIONS	Preventive measures	Reinforce water towers and welds Remove sources of potential flying debris Design new facilitites, control rooms and offices to withstand high winds Backup transformer units Expanding the generation reserve capacity (e.g. deploying additional Emergency generators Protection system	Backup transformer units Technical choises Parallel lines Maintenance of electric components Emergency generators Protection system	Remove debris, trees or other fire -hazard materials Institute high fire danger procedures such as smoking -Install fire resilient building mate - Modify treatment process for sediment in water Emergency generators Protection system	Use tronger overhead line poles Installing multiple circuits in parallel Parallel lines Maintenance of electric components Emergency generators Protection system	Elevate or protect electrical service plans (e.g. substations) Upsize culverts to better handle flood surges Replace pumps with submersible or inline pumps Relocate equipment outside Waterprof control rooms Important systems in low risk zones Distributed generation Emergency generators	Remove debris, trees or other fire - hazard materials Institute high fire danger procedures such as smoking bans and fire bans -Install fire resilient building materials - Modify treatment process for sediment in water Protection system
	Corrrective measures	Protection & Isolation system Regulation services Secure generators against Wind activity Purchase or rent a backup power generator	Protection & Isolation system Regulation services	Protection & Isolation system Regulation services	Protection & Isolation system Regulation services Secure generators against Wind activity	Protection & Isolation system Regulation services Secure generators against water activity	Protection & Isolation system Regulation services
	Restorative Measures	Data availability	Data availability Technological update	Data availability Technological update	Data availability Technological update	Data availability Technological update	Data availability

Figure 20. Preventive, corrective, and restorative mitigation actions



											Interested systems		
	Mitigation Actions	Earthquake	Tsunami	Eruption	Landslide	Storms	Lightning	Heat-wave	Floods		Generation	Transmission and distribution netowrks	Consumers
Preventive measures	Risk mask	X	X	X					X		X	X	X
	Important systems in low risk zones	X	X	X					X		X		X
	Technical choises	X				X	X		X		X	X	X
	Redundancy (meshed grid)	X	X	X	X	X	X	X	X		X	X	X
	Parallel lines					X	X				X	X	X
	Distributed generation	X	X	X					X		X		
	Components maintenance					X	X		X		X	X	X
	Environment maintenance				X	X	X	X	X		X	X	X
	Emergency generators	X	X	X	X	X	X	X	X				X
	Protection system	X	X	X	X	X	X	X	X		X	X	X
	Measurement system	X	X	X	X	X	X	X	X		X	X	X
	Regulation services	X	X	X	X	X	X	X	X		X	X	X
Corrective measures	Protection system	X	X	X	X	X	X	X	X		X	X	X
	Regulation services	X	X	X	X	X	X	X	X		X	X	X
Restoration measures	Data availability	X	X	X	X	X	X	X	X		X	X	X
	Technological update	X			X	X	X	X	X		X	X	X
	Regulation services	X	X	X	X	X	X	X	X		X	X	X

Figure 21. Correlation between mitigation actions and hazards & EPES main components

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

3.1.4 Power system frequency control and power oscillation detection methods

In addition to the identified resilience actions in the previous section, it is crucial to investigate frequency control on low inertia power grids and vulnerability to interarea oscillations to increase the resilience of future power systems.

3.1.4.1 Frequency control on low inertia power grids

A brief summary of the state-of-the-art review can be found in Annex V: Resilience actions, which gives an overview of the latest measures to improve resiliency in low-inertia power systems. This section reports a description of the resilience mitigation actions regarding the frequency control on low-inertia power grids.

Threat identification

Due to the reduction of system inertia that goes along with the increasing penetration level of RES, power grids are much more vulnerable to higher ROCOF and larger frequency deviation. As many countries will increase their share of RES, the threat of frequency instability becomes increasingly significant. For example, according to the German Renewable Energies Act (*Latest Version EEG 2023*, 2023), renewable energies are to account for 80 % of gross electricity consumption in 2030.

ROCOF protection relays protect synchronous generators from damage caused by high ROCOF values by disconnecting the generator from the grid, resulting in a loss of generation. This reaction can, in turn, worsen the ROCOF value. This has the potential to initiate further cascade tripping events, leading to load shedding, system islanding, or system blackouts. On the other hand, if ROCOF-protection relays would fail to disconnect, pole slipping could be the consequence, which can cause severe mechanical stresses within the generator and ultimately lead to the complete destruction of the generator and massive instability on the grid.

Mitigation and countermeasure actions categorization

For the identification of the mitigation actions, a categorization process of the possible countermeasures is reported:

a. Location of the measure within the supply chain

b. Response times

c. Status of technological development of the countermeasures

d. The extent of use in current power systems

e. Potential future expansion and limits of the application of the countermeasure

Mitigation actions

Finally, a description of countermeasures and underlying principles sorted along resilience phases is reported (Shazon et al., 2022):

Prevention

a. Adaption of the amount of physical inertia in the network by

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

   i. Limitation or reduction of the instantaneous penetration of RES that does not provide virtual inertia by curtailing their production so that a higher share of conventional generation or energy sources providing virtual inertia is connected at a given time.

   ii. Increasing the number of conventional generation units connected at a given time but decreasing their individual power output.

b. Expanding the utilization of hidden inertia emulation from wind plants: Thereby, the kinetic energy stored in the (asynchronous) rotating mass can be extracted using additional control loops.

c. Introduction of the requirement of Photovoltaics (PV) / Wind Power Plant (WPP) de-loading operation mode: Thereby, the PV/WPP is not operated in the maximum power point and therefore creates a reserve that can be utilized during a contingency.

d. Introduction of the requirement of Delta Power Control (DPC): Thereby, the active output power of the PV is curtailed in order to provide a reserve that can be utilized during a contingency. This can be achieved by dissipating or storing the reserve power in normal operation modes.

e. Synchro-converters that mimic the inertial behavior of synchronous generators by following the swing equation.

f. Inverters mimic the load frequency relief characteristics of induction machines and, thus, contribute to frequency regulation.

Preparation

Predicting the frequency nadir and ROCOF value before an event for hypothetical disruptions can be used in the planning phase of the system operators. Corresponding actions can be taken, such as the preparation of additional reserves, i.e., bringing in more rotating mass to increase system inertia.

Response

Prediction of the nadir during an event enables to optimize the response phase. For example, if the prediction shows that the frequency will fall below UFLS limits, system operators do not have to wait until the frequency reaches these limits, but they can shed load earlier and hence, more effectively.

The frequency prediction can be obtained via a bottom-up approach, which starts by using the information that is available at each unit of the system. Then, this information is scaled up to provide a (dynamic) system representation.

3.1.4.2 Interarea oscillation vulnerability and resilience actions

Interarea oscillations occur due to the interaction between different regions or groups of generators in the power system. These oscillations usually arise when there is a high-power flow transfer across weak interconnections or when there are high-gain exciters in the system. Interarea oscillations typically occur at low frequencies, in the range of 0.1 to 0.7 Hz, and are more challenging to analyse and control compared to local mode oscillations (in the range of 0.7 to 2 Hz), which happen within a single generator (Kundur

& Balu, 1994). The presence of interarea oscillations can cause stability issues in a power system and lead to failures, such as line tripping, network splitting, generator outages, and even blackouts (Biyik & Husein, 2018; Klein et al., 1991). More details about resilience actions regarding the interarea oscillations can be found in Annex V: Resilience actions.

3.2 Cyber Layer

3.2.1 Main goals and objectives

In National Institute of Standards and Technology (NIST) SP 800-160 Volume 2 (Ross et al., 2018), cyber resiliency is defined as: *"the ability to anticipate, withstand, recover from, and adapt to adverse conditions, stresses, attacks, or compromises on systems that use or are enabled by cyber resources …".* The relevant question is how cyber resilience differs from cybersecurity. In literature, the difference has sometimes been a bit artificial. In essence, the focus of resilience is more on the behaviour of the system under stress, whereas security refers to the state of being free (or protected) from danger or threats. Nowadays, a good cybersecurity program also includes security controls to detect, respond and recover from cyber-attacks and to respond to new threats and vulnerabilities proactively. This study will not distinguish between cybersecurity controls or cyber resilience actions, but rather focus on operational actions at the cyber layer of EPES to increase resilience against cyber-attacks. These so-called *operational cyber resilience actions* are becoming more important due to the growing cyber threat and the increase of the cyber-attack surface of EPES due to the energy transition and associated digitalization. Furthermore, the growing cyber threat and greater dependency of society on digital systems drive new cybersecurity regulations for operators of critical infrastructure, including EPES operators. In particular, the Network and Information Security 2 (NIS) directive and the Network Code on Cybersecurity will require EPES operators in the European Union to comply with security rules to increase the level of cyber-resilience.

The goal of this study is to:

- Identify *operational cyber resilience actions.* These include actions to detect and respond to cyber-attacks and proactive actions to reduce the cyberattack surface when new threats and vulnerabilities.
- Identify the *technical and procedural controls and capabilities* to enable these operational cyber resilience actions.
- Identify the *constraints and decision-making criteria* for these operational cyber resilience actions in the EPES environment.

Approach:

- Assess state-of-the-art, particularly cybersecurity control frameworks, standards, and literature related to operational cybersecurity and cyber resilience.
- Conduct interviews and workshops with cybersecurity experts working in the EPES domain.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

- Compile a set of *operational cyber resilience actions* with guidance for decision-making and on the capabilities to enable these actions.

3.2.2 State of the Art

For the state of the art on operational cyber resilience actions, it is relevant to distinguish between the different stages of a system's lifecycle, particularly between design time which is related to development and production, and run time which is mostly concerned with operation and maintenance. The discipline of designing systems with the ability to anticipate, withstand, recover from, and adapt to cyber-attacks is cyber resilience engineering. Over the last couple of years, several guidance documents and frameworks have been developed to support organizations with the design of cyber-resilient systems. Most notable are the NIST SP 800-160, Volume 2 (Rev. 1) (Ross et al., 2018) and CREF Navigator™ from MITRE (*CREF Navigator*, n.d.).

For guidance on *operational* cyber resilience actions during run time, the traditional cybersecurity control frameworks provide a good foundation. The most well-known is the ISO/IEC 27000 series (ISO/IEC JTC 1/SC 27, 2022) for Information Security Management System (ISMS). The ISO/IEC 27002:2022 (ISO, 2022) provides a reference set of generic information security controls. A sector-specific extension of ISO/IEC 27002 for the energy utility industry is available as ISO/IEC27019:2017 (ISO, 2016). This standard provides energy utility-sector–specific security control objectives and controls for controlling and monitoring the production or generation, transmission, storage, and distribution of electric power, gas, oil, and heat and for the control of associated supporting processes. Note that this standard is at the moment of writing under revision.

Within the Industrial Automation and Control System (IACS), it is more common to apply the IEC 62443 series of standards[5]. This is a multi-part set of standards to improve the safety, integrity, availability, and confidentiality of components or systems used for automation and control. Part 2-1 of the IEC 62443 specifies security program requirements for asset owners of IACS (IEC TC 65, 2023). Operators of EPES can use the IEC 62443-2-1 to support implementing and maintaining procedural, personnel, and technology-based capabilities to reduce the cybersecurity risk of their IACS.

Last but not least, NIST has published a draft guide to OT under the number NIST SP 800-82 Rev. 3 (Stouffer et al., 2022). This document provides guidance on the security of OT systems while addressing performance, reliability, and safety requirements that are typical in OT environments and can support the definition of *operational cyber resilience actions*.

The responsibility for the execution of o*perational* cyber resilience actions typically lies within the so-called Security Operations Centre (SOC) and Computer Security Incident Response Team (CSIRT). Within an EPES environment, this responsibility will be shared with the OT control room. There is not much guidance on combined IT / OT SOCs and collaboration of SOC with OT control room. There are guidance documents on establishing a SOC and/or CSIRT (Knerler, 2022), (Kossakowski, K. P., 2019), (Taurins, E, 2020) and establishing incident response, such as ISO/IEC 27035 standard series (ISO, 2023).

3.2.3 Resilience actions

As acknowledged in regulatory and industry state-of-art, cyber resilience engineering in EPES cannot simply be ported form information technology environments and must consider aspects specific to operational technologies environments. The focus of resilience actions at the cyber layer is on enabling the operational resilience of EPES against cyber-attacks.

The ISO/IEC 27002:2022, IEC 62443-2-1(IEC TC 65, 2023, p. 62443), NIST 800-82r3, and 11 Strategies of a World-Class security operations centre are studied. For each document, the EPES-specific cyber resilience approaches and considerations are identified. All collected notions into actions to anticipate, withstand, recover from, and adapt to adverse conditions are clustered. In the following paragraphs, we present the categories of identified cyber resiliency actions for EPES, divided per resiliency goals according to the NIST resiliency engineering framework (Ross et al., 2018): anticipate, withstand, recover, and adapt. Figure 22 contextualizes the scope of each cyber resilience action with respect to a typical timeline of a security incident.

Further considerations on the high-level preconditions for an EPES organization to adopt cybersecurity resiliency actions are provided. Finally, the automation trends in relation to the cybersecurity resiliency goals are summarized.

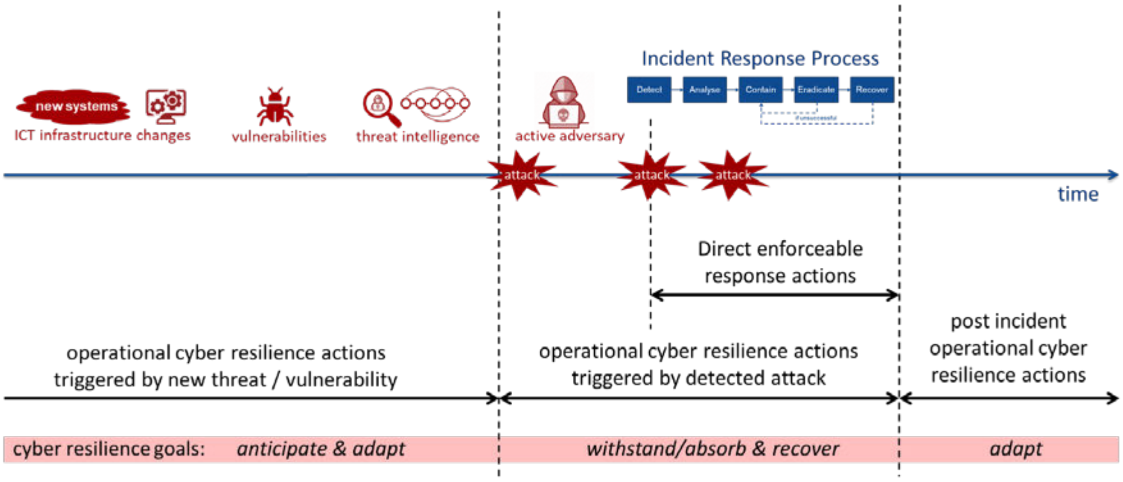

Incident Response Process
Detect
Analyse
Contain
Eradicate
Recover
if unsuccessful
new systems
ICT infrastructure changes
vulnerabilities
threat intelligence
active adversary
attack
attack
attack
time
Direct enforceable response actions
operational cyber resilience actions triggered by new threat / vulnerability
operational cyber resilience actions triggered by detected attack
post incident operational cyber resilience actions
cyber resilience goals: anticipate & adapt
withstand/absorb & recover
adapt

Figure 22. Visualization of the distinction between the two types of operational cyber resilience actions

3.2.3.1 Anticipate

The anticipation goal is to establish a robust cybersecurity posture against cyber threats. Anticipate plays a major role in a number of resiliency actions that can be undertaken. From a robust cybersecurity posture comes greater effectiveness in withstanding, recovering, and adapting to adverse cyber events. In the following, the emerging categories of resiliency actions to anticipate cyber threats are enumerated.

Assets inventory:

Paramount to protecting an EPES infrastructure is a clear understanding of what the infrastructure looks like and what it should look like[6]. To this end, the infrastructure should be inventoried both at the hardware and layer of OT and IT systems and at the software

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

components layer. A continuous verification and update of EPES Bills of Materials (BoM) is fundamental to making the infrastructure resilient.

Governance:

It is fundamental that a SOC has the authority to operate in an EPES environment such that it can effectively assist in responding to cyber threats without delays. This should be established with clear planning of the cybersecurity roles within the infrastructure and establishing procedures such that the SOC can cooperate and exchange information with OT personnel. For instance, a SOC should have Points of Contact (PoCs) at manned remote locations of the EPES infrastructure to have a direct line of communication to assess status and intervention needs. An effective and clear establishment of a SOC and its operations in an EPES organization directly determines its resiliency to cyber threats.

Threat Intelligence monitoring:

An EPES organization must establish a process to continuously monitor the landscape of cyber threats, to understand what attacks it may face, and hence fine-tune the risk strategy. This helps an EPES organization dynamically and effectively adjust its cyber defenses. For instance, a surge in ransomware may lead an EPES organization to administer backups; and the emergence of a threat group leveraging specific vulnerabilities may lead to addressing vulnerable systems within an EPES infrastructure.

Infrastructure monitoring:

An EPES organization should maintain a dynamic, up-to-date, and as-complete-as-possible situational awareness of the status of the assets and their interconnections. This is achieved via establishing sensors, data streams, and logs. Such data should be provided to event and anomaly detection processes to be able to identify the emergence of anomalies immediately.

Planning: risk management, response, recovery:

EPES organizations should perform pre-emptive assessments and plannings with regard to the following aspects:

- Identification of priority assets and processes with respect to safety, availability, integrity, and confidentiality.
- Establishment of elements of cyber risks to safety, availability, integrity, and confidentiality of processes and assets – including supply chain.
- Planning of procedures to address cyber risks (e.g., cooperation with suppliers, deployment of protective measures, etc.)
- Procedures to respond to cyber intrusions or attacks, planned according to different attack scenarios, use cases, and the severity of the attacks.
- Procedures to recover from cyber-attacks once the cyber-threats have been addressed.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Protective measures:

Protective cyber measures should be employed in an EPES environment according to the risk management strategy of the EPES authority and to guarantee baseline protection of safety, availability, integrity, and confidentiality. Protective measures concern elements such as backups; authentication and access control cyber-physical infrastructures; cybersecurity awareness training for EPES employees; data security practices, including encryption and integrity of data through its life cycle; protective technologies such as firewalls, canary detectors, honeypots, data diodes, (network) intrusion prevention and detection systems, etc.

Protective measurements are of utmost importance on the infrastructure monitoring and control elements, as they are the primary source of data for grid operators, and they also allow the operation of the electric infrastructure, including transformers and breakers. As these elements are normally widely interconnected within the grid, they could be a potential entry point used by cyber-attackers to disturb the normal operation of the electric grid. Other examples of cyber-attacks for these elements are denial of service, man in the middle, data spying, manipulation, and deletion of data. Against these cyber-attacks, the are several policies/techniques to be used in sensors and other monitoring and control elements to enhance their resilience: securing access control, hardening on non-used ports, secured communications, secured design rules, security logging, or backup/restore policies, among others.

3.2.3.2 Withstand

The withstand resiliency goal aims at establishing the actions and procedures to take during the activity of a cyber-attack or intrusion, such that damages and degradation of safety, availability, integrity, and confidentiality are limited. Resiliency actions to withstand cyber-attacks from ISO/IEC 27002:2022, the IEC 62443-2-1, the NIST 800-32r3, and the 11 Strategies of a World-Class Security Operation Center are categorized in the following.

Monitoring and detection:

An EPES organization should be able to monitor the status of EPES assets and their interconnections for several reasons, among which: detect cyber-attacks and intrusions; understand how such attacks and intrusions spread to control the situation insofar as possible dynamically; record the forensics of a cyber incident for evidence and post-study.

Response actions:

A SOC or a CSIRT should be able to perform response actions according to the planned response to adverse cyber events. Response teams should analyze how the cyber threat manifests, determine its severity, and the actions possible to Marginate it. In this sense, it is paramount to establish effective lines of communication between IT and OT teams. Along the response process, the EPES organizations should maintain and curate communications with all stakeholders interested in the cyber-attack, including authorities, clients, and suppliers, and perform reporting of the response activities.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Maintenance of availability and safety:

According to a response plan, actions should be taken such that the availability and safety of critical services is prioritized, hence safeguarded to the maximum extent possible.

3.2.3.3 Recover

Recovery resilience actions aim at reestablishing a fully operational status of an EPES organization following the eradication of a cyber threat. As per response actions, recovery actions should also be timely communicated to all interested stakeholders. As recovery actions may require the installation of security patches or otherwise additional protective measures, it is important that such interventions are performed in a safe manner.

3.2.3.4 Adapt

Adaptation as a resilience action aims at dynamically changing aspects of the EPES organization and cybersecurity posture to better protect against cyber adversaries. Adaptation actions may follow a security incident or threat intelligence received from the defender's community (other EPES companies, threat intelligence agencies, or security research).

Identify improvements:

The acquisition of a more mature understanding of the cyber threats' context, and its own security posture, should prompt an EPES organization to identify improvements that could be enacted in planned security procedures, posture maintenance (protective measures), response, and recovery. A dedicated process for the identification and application of improvements would make an EPES company more resilient to cyber threats.

Information sharing:

In the same context, an EPES organization should share the valuable insights in cybersecurity management learned from preparing for, withstanding, and recovering from an adverse cyber event. EPES organizations should present such insights to the defender's community in a clear and re-actionable way to further the resiliency of the whole industry sector.

3.2.4 Preconditions for cyber resilience actions

EPES organizations need to address certain preconditions in order to take actions to increase resiliency to cyber-attacks, in particular concerning organizational culture, personnel, and connection between IT and OT assets.

EPES organizations should embrace a cybersecurity culture, understanding that, per the current technological landscape, OT cybersecurity and safety are sides of the same medal. Cybersecurity personnel should participate in organizational decisional processes and be able to coordinate with management and OT personnel to promote and secure a solid cybersecurity posture in consideration of emerging risks.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

It is fundamental that both cybersecurity and OT teams are able to understand each other. OT personnel must understand the cyber-risks related to OT environments as they are connected to IT environments. Cybersecurity personnel must be educated about the OT domain, the specific procedures and technologies that characterize it, their operational requirements, and their limitations.

Overall, it is non-renounceable that connections between IT and OT environments are thoroughly designed, understood, monitored, and controlled in a way aligned with the EPES organization risk strategy.

3.2.4.1 Automation landscape

The growing complexity of digital systems and advancements in cyber-attacks prompts a demand and opportunity to develop technology to automate defense operations. Market and research provide several tools that support the accomplishment of cyber resilience actions.

Software and hardware BoMs have become mandatory for EPES organizations to address supply chain and component security management. Tools offer network and software scanning, automatically populate BoM, or offer automated support for risk assessment processes (Ehrlich et al., 2022). With registries for hardware and software assets, it is possible to generate models of IT/OT infrastructures that represent dependencies and relationships.

Such models can be enriched automatically with telemetry data coming from communication links and sensors. It is thus possible to automatically generate a dynamic and up-to-date representation of the digital assets of an EPES organization – digital twins. Besides providing situational awareness, digital twins can be used to forecast the status of operations following adverse events automatically. As the forecast of impact can be automated, so can the elaboration of remedy operations.

In turn, modern networking approaches such as Software Defined Networking (SDN), though born in the IT context, can also be employed in IT-OT environments (Foschini et al., 2021) and offer dynamic reconfiguration capabilities. Emerging Security Orchestration, Automation, and Response (SOAR)-serving standards and capabilities facilitate sharing Courses of Actions (CoA) across stakeholders to respond to specific threats, with the opportunity of automating several steps (Mir & Ramachandran, 2021).

With dynamic reconfiguration, systems or network segments can be semi or automatically restricted in response to detected threats. Similarly, automated actions can be taken in response to the publication of relevant threat intelligence, for instance, a new vulnerability affecting a historian server.

A digital twin of an EPES organization that supports scenario injection, forecasting, and automated remedy, it greatly supports resiliency against cyber-attacks.

Where many opportunities for automation exist, it is paramount that automation for EPES cybersecurity operations is carefully planned, evaluated, and deployed only where there is the absolute certainty that it does not interfere with the critical availability and safety of OT systems. On the other hand, automated reasoning in OT can offer support, guidance, and option awareness to human operators.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

4 Conclusion

The report delves into understanding the critical problem of cascading failures within modern power systems. By analysing pre-conditions and initiating events and investigating the main stages and underlying mechanisms of cascading failures, critical factors contributing to these failures are identified. The report also sheds light on how cyber-attacks can exploit these critical factors to initiate or accelerate cascading failures, and the impact of such attacks is demonstrated through simulation scenarios.

Furthermore, the report proposes strategies to enhance resilience at the physical and cyber system layers and minimize economic losses in modern power systems. By implementing these measures, power systems can be better safeguarded against power outages and blackouts, reinforcing their stability and reliability.

In conclusion, this report emphasizes the need to address cascading failures and improve resilience in modern power systems. By adopting the proposed strategies and understanding the interplay between physical and cyber layers, power system operators can better cope with challenges and ensure the continuous electricity supply. Ultimately, this comprehensive report offers valuable insights for system operators, policymakers, and researchers working towards a more robust and secure power grid.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

References

Acharya, S., Dvorkin, Y., & Karri, R. (2020). Public Plug-in Electric Vehicles + Grid Data: Is a New Cyberattack Vector Viable? *IEEE Transactions on Smart Grid*, *11*(6), 5099–5113. https://doi.org/10.1109/TSG.2020.2994177

Amini, S., Pasqualetti, F., & Mohsenian-Rad, H. (2018). Dynamic Load Altering Attacks Against Power System Stability: Attack Models and Protection Schemes. *IEEE Transactions on Smart Grid*, *9*(4), 2862–2872. https://doi.org/10.1109/TSG.2016.2622686

Baldick, R., Chowdhury, B., Dobson, I., Dong, Z., Gou, B., Hawkins, D., Huang, Z., Joung, M., Kim, J., Kirschen, D., Lee, S., Li, F., Li, J., Li, Z., Liu, C.-C., Luo, X., Mili, L., Miller, S., Nakayama, M., … Zhang, X. (2009). Vulnerability assessment for cascading failures in electric power systems. *2009 IEEE/PES Power Systems Conference and Exposition*, 1–9. https://doi.org/10.1109/PSCE.2009.4839939

Bhavaraju, M. P., & Nour, N. E. (1992). *TRELSS: A computer program for transmission reliability evaluation of large-scale systems* (EPRI-TR-100566-Vol.2). Electric Power Research Inst., Palo Alto, CA (United States); Public Service Electric and Gas Co., Newark, NJ (United States). https://www.osti.gov/biblio/5210172

Biyik, E., & Husein, M. (2018). Damping wide-area oscillations in power systems: A model predictive control design. *TURKISH JOURNAL OF ELECTRICAL ENGINEERING & COMPUTER SCIENCES*, *26*, 467–478. https://doi.org/10.3906/elk-1705-247

Bompard, E., Huang. T., Tenconi. A., Wu. Y., Zelastiba. D., Cremenescu. M., et al. (2011). *Securing the European Electricity Supply Against Malicious and accidental thrEats | SESAME | Project | Fact sheet | FP7 | CORDIS | European Commission*. https://cordis.europa.eu/project/id/261696

Brasinika, D. (2023). *Characterization and classification of EPES threats*. Horizon Europe.

Broderick, C. (2016). *Parameters related to frequency stability*.

Broderick, C. (2018a). Limited frequency sensitive mode. *ENTSOE*.

Broderick, C. (2018b). *Need for synthetic inertia (SI) for frequency regulation*.

Broderick, C. (2018c). *Rate of Change of Frequency (RoCoF) withstand capability*.

Chadwick, J. E. (2013). How a smarter grid could have prevented the 2003 U.S. cascading blackout. *2013 IEEE Power and Energy Conference at Illinois (PECI)*, 65–71. https://doi.org/10.1109/PECI.2013.6506036

Chen, B., Pattanaik, N., Goulart, A., Butler-purry, K. L., & Kundur, D. (2015). Implementing attacks for modbus/TCP protocol in a real-time cyber physical system test bed. *2015 IEEE International Workshop Technical Committee on Communications Quality and Reliability (CQR)*, 1–6. https://doi.org/10.1109/CQR.2015.7129084

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Cheng, Y., Huang, S.-H., Rose, J., Pappu, V. A., & Conto, J. (2016). ERCOT subsynchronous resonance topology and frequency scan tool development. *2016 IEEE Power and Energy Society General Meeting (PESGM)*, 1–5. https://doi.org/10.1109/PESGM.2016.7741951

Chitturi, S., Chakrabarti, S., & Singh, S. N. (2014). Comparing performance of Prony analysis and matrix pencil method for monitoring power system oscillations. *2014 IEEE Innovative Smart Grid Technologies - Asia (ISGT ASIA)*, 447–452. https://doi.org/10.1109/ISGT-Asia.2014.6873833

Cimellaro, G. P., Reinhorn, A. M., & Bruneau, M. (2010). Seismic resilience of a hospital system. *Structure and Infrastructure Engineering*, *6*(1–2), 127–144. https://doi.org/10.1080/15732470802663847

Climate Central. (2022). *Surging Power Outages and Climate Change | Climate Central*. https://www.climatecentral.org/report/surging-power-outages-and-climate-change

Corsi, S., & Sabelli, C. (2004). General blackout in Italy Sunday September 28, 2003, h. 03:28:00. *IEEE Power Engineering Society General Meeting, 2004.*, 1691–1702. https://doi.org/10.1109/PES.2004.1373162

CREF Navigator. (n.d.). Retrieved August 21, 2023, from https://crefnavigator.mitre.org/about

Dabrowski, A., Ullrich, J., & Weippl, E. R. (2017). Grid Shock: Coordinated Load-Changing Attacks on Power Grids: The Non-Smart Power Grid is Vulnerable to Cyber Attacks as Well. *Proceedings of the 33rd Annual Computer Security Applications Conference*, 303–314. https://doi.org/10.1145/3134600.3134639

Dobson, I., Carreras, B. A., & Newman, D. E. (2005). Branching Process Models for the Exponentially Increasing Portions of Cascading Failure Blackouts. *Proceedings of the 38th Annual Hawaii International Conference on System Sciences*, 64a–64a. https://doi.org/10.1109/HICSS.2005.125

Ehrlich, M., Lukas, G., Trsek, H., Jasperneite, J., & Diedrich, C. (2022). Investigation of Resource Constraints for the Automation of Industrial Security Risk Assessments. *2022 IEEE 18th International Conference on Factory Communication Systems (WFCS)*, 1–8. https://doi.org/10.1109/WFCS53837.2022.9779174

Ember's analysis. (2022, February 1). *European Electricity Review 2022*. Ember. https://ember-climate.org/insights/research/european-electricity-review-2022/

ENTSO-E SG SPD REPORT. (2017, July 13). *ANALYSIS OF CE INTER-AREA OSCILLATIONS OF 1 ST DECEMBER 2016*. Https://Www.Entsoe.Eu/. https://eepublicdownloads.entsoe.eu/clean-documents/SOC%20documents/Regional_Groups_Continental_Europe/2017/CE_inter-area_oscillations_Dec_1st_2016_PUBLIC_V7.pdf

Eremia, M., & Shahidehpour, M. (2013). Handbook of Electrical Power System Dynamics: Modeling, Stability, and Control. *SYSTEM DYNAMICS*. https://doi.org/10.1002/9781118516072

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Eto, J. (2004). *Final Report on the August 14, 2003 Blackout in the United States and Canada: Causes and Recommendations*. U.S.-Canada Power System Outage Task Force.

Foschini, L., Mignardi, V., Montanari, R., & Scotece, D. (2021). An SDN-Enabled Architecture for IT/OT Converged Networks: A Proposal and Qualitative Analysis under DDoS Attacks. *Future Internet*, *13*(10), 258. https://doi.org/10.3390/fi13100258

Foyen, S., Kvammen, M.-E., & Fosso, O. B. (2018). Prony's method as a tool for power system identification in Smart Grids. *2018 International Symposium on Power Electronics, Electrical Drives, Automation and Motion (SPEEDAM)*, 562–569. https://doi.org/10.1109/SPEEDAM.2018.8445308

Greer, C., Wollman, D. A., Prochaska, D., Boynton, P. A., Mazer, J. A., Nguyen, C., FitzPatrick, G., Nelson, T. L., Koepke, G. H., Jr, A. R. H., Pillitteri, V. Y., Brewer, T. L., Golmie, N. T., Su, D. H., Eustis, A. C., Holmberg, D., & Bushby, S. T. (2014). NIST Framework and Roadmap for Smart Grid Interoperability Standards, Release 3.0. *NIST*. https://www.nist.gov/publications/nist-framework-and-roadmap-smart-grid-interoperability-standards-release-30

Guo, H., Zheng, C., Iu, H. H.-C., & Fernando, T. (2017). A critical review of cascading failure analysis and modeling of power system. *Renewable and Sustainable Energy Reviews*, *80*, 9–22. https://doi.org/10.1016/j.rser.2017.05.206

Guo, Q., Xin, S., & Wang, J. (2016). Comprehensive security assessment for a cyber physical energy system: A lesson from Ukraine's blackout. *Dianli Xitong Zidonghua/Automation of Electric Power Systems*, *40*, 145–147. https://doi.org/10.7500/AEPS20160113101

Haes Alhelou, H., Hamedani-Golshan, M., Njenda, T., & Siano, P. (2019). A Survey on Power System Blackout and Cascading Events: Research Motivations and Challenges. *Energies*, *12*(4), 682. https://doi.org/10.3390/en12040682

Hatziargyriou, N., Milanović, J., Rahmann, C., Ajjarapu, V., Canizares, C. A., Erlich, I., Hill, D., Hiskens, I., Kamwa, I., Pal, B. C., Pourbeik, P., Sanchez-Gasca, J., Stankovic, A. M., Van Cutsem, T., Vittal, V., & Vournas, C. (2020). *Stability Definitions and Characterization of Dynamic Behavior in Systems with High Penetration of Power Electronic Interfaced Technologies*.

Hatziargyriou, N., Milanovic, J., Rahmann, C., Ajjarapu, V., Canizares, C., Erlich, I., Hill, D., Hiskens, I., Kamwa, I., Pal, B., Pourbeik, P., Sanchez-Gasca, J., Stankovic, A., Van Cutsem, T., Vittal, V., & Vournas, C. (2021). Definition and Classification of Power System Stability – Revisited & Extended. *IEEE Transactions on Power Systems*, *36*(4), 3271–3281. https://doi.org/10.1109/TPWRS.2020.3041774

Huang, B., Cardenas, A. A., & Baldick, R. (2019a). *Not Everything is Dark and Gloomy: Power Grid Protections Against {IoT} Demand Attacks*. 1115–1132. https://www.usenix.org/conference/usenixsecurity19/presentation/huang

Huang, B., Cardenas, A. A., & Baldick, R. (2019b). *Not Everything is Dark and Gloomy: Power Grid Protections Against {IoT} Demand Attacks*. 1115–1132. https://www.usenix.org/conference/usenixsecurity19/presentation/huang

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

IEC TC 65. (2023). *Industrial communication networks—Network and system security—Part 2-1: Establishing an industrial automation and control system security program*. https://webstore.iec.ch/publication/7030

ISO. (2016, August 15). *ISO/IEC 27019:2017*. ISO. https://www.iso.org/standard/68091.html

ISO. (2022). *ISO/IEC 27002:2022*. ISO. https://www.iso.org/standard/75652.html

ISO. (2023). *ISO/IEC 27035-1:2023*. ISO. https://www.iso.org/standard/78973.html

ISO/IEC JTC 1/SC 27. (2022, May 4). *ISO/IEC 27000:2018*. ISO. https://www.iso.org/standard/73906.html

ISO/TC 262 Risk management. (2019, July 1). *Risk management—Risk assessment techniques*. ISO. https://www.iso.org/standard/72140.html

Jacobs, N., Hossain-McKenzie, S., & Vugrin, E. (2018). Measurement and Analysis of Cyber Resilience for Control Systems: An Illustrative Example. *2018 Resilience Week (RWS)*, 38–46. https://doi.org/10.1109/RWEEK.2018.8473549

Klein, M., Rogers, G. J., & Kundur, P. (1991). A fundamental study of inter-area oscillations in power systems. *IEEE Transactions on Power Systems*, *6*(3), 914–921. https://doi.org/10.1109/59.119229

Knerler, K. (2022). *11 Strategies of a World-Class Cybersecurity Operations Center*.

Kossakowski, K. P. (2019). *CSIRT Services Framework Version 2.1*. FIRST — Forum of Incident Response and Security Teams. https://www.first.org/standards/frameworks/csirts/csirt_services_framework_v2.1

Kosterev, D. N., Taylor, C. W., & Mittelstadt, W. A. (1999). Model validation for the August 10, 1996 WSCC system outage. *IEEE Transactions on Power Systems*, *14*(3), 967–979. https://doi.org/10.1109/59.780909

Kundur, P., & Balu, N. J. (1994). *Power System Stability and Control*. McGraw-Hill.

Kundur, P., Paserba, J., Ajjarapu, V., Andersson, G., Bose, A., Canizares, C., Hatziargyriou, N., Hill, D., Stankovic, A., Taylor, C., Van Cutsem, T., & Vittal, V. (2004). Definition and classification of power system stability IEEE/CIGRE joint task force on stability terms and definitions. *IEEE Transactions on Power Systems*, *19*(3), 1387–1401. https://doi.org/10.1109/TPWRS.2004.825981

Latest version EEG 2023—Climate Change Laws of the World. (2023). https://climate-laws.org/document/renewable-energy-sources-act-eeg-latest-version-eeg-2022_1b40

Li, B., & Sansavini, G. (2017). Energy markets impact on the risk of cascading failures in power systems. *2017 14th International Conference on the European Energy Market (EEM)*, 1–6. https://doi.org/10.1109/EEM.2017.7981958

Li, J., Liu, H., Bi, T., & Ma, S. (2018). A spectral line curve fitting based algorithm for inter-harmonics measurement. *2018 IEEE 2nd International Electrical and Energy Conference (CIEEC)*, 100–104. https://doi.org/10.1109/CIEEC.2018.8745945

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Liang, G., Zhao, J., Luo, F., Weller, S. R., & Dong, Z. Y. (2017). A Review of False Data Injection Attacks Against Modern Power Systems. *IEEE Transactions on Smart Grid*, *8*(4), 1630–1638. https://doi.org/10.1109/TSG.2015.2495133

Mei, S., He, F., Zhang, X., Wu, S., & Wang, G. (2009). An Improved OPA Model and Blackout Risk Assessment. *IEEE Transactions on Power Systems*, *24*(2), 814–823. https://doi.org/10.1109/TPWRS.2009.2016521

Mir, A. W., & Ramachandran, R. K. (2021). Implementation of Security Orchestration, Automation and Response (SOAR) in Smart Grid-Based SCADA Systems. In S. S. Dash, B. K. Panigrahi, & S. Das (Eds.), *Sixth International Conference on Intelligent Computing and Applications* (pp. 157–169). Springer. https://doi.org/10.1007/978-981-16-1335-7_14

Mohsenian-Rad, A.-H., & Leon-Garcia, A. (2011). Distributed Internet-Based Load Altering Attacks Against Smart Power Grids. *IEEE Transactions on Smart Grid*, *2*(4), 667–674. https://doi.org/10.1109/TSG.2011.2160297

Narendra, K., Fedirchuk, D., Midence, R., Zhang, N., Mulawarman, A., Mysore, P., & Sood, V. (2011). New microprocessor based relay to monitor and protect power systems against sub-harmonics. *2011 IEEE Electrical Power and Energy Conference*, 438–443. https://doi.org/10.1109/EPEC.2011.6070241

Ndreko, M. (TenneT). (2021). *FREQUENCY RANGES*.

Nedic, D. P., Dobson, I., Kirschen, D. S., Carreras, B. A., & Lynch, V. E. (2006). Criticality in a cascading failure blackout model. *International Journal of Electrical Power & Energy Systems*, *28*(9), 627–633. https://doi.org/10.1016/j.ijepes.2006.03.006

Ning Zhou, Zhenyu Huang, & Matthew Hauer. (2010, August). *FINAL PROJECT REPORT OSCILLATION DETECTION AND ANALYSIS*. Pacific Northwest National Laboratory. https://escholarship.org/content/qt4z76h1cn/qt4z76h1cn_noSplash_55946ed634d2eea266fe9bdcbc5f67e7.pdf

Panda, S., Baliarsingh, A. K., Mahapatra, S., & Swain, S. C. (2016). Supplementary damping controller design for SSSC to mitigate sub-synchronous resonance. *Mechanical Systems and Signal Processing*, *68–69*, 523–535. https://doi.org/10.1016/j.ymssp.2015.07.013

Parfomak, P. W. (2014). *Physical Security of the U.S. Power Grid: High-Voltage Transformer Substations*.

Paul, S., Ding, F., Utkarsh, K., Liu, W., O'Malley, M. J., & Barnett, J. (2022). On Vulnerability and Resilience of Cyber-Physical Power Systems: A Review. *IEEE Systems Journal*, *16*(2), 2367–2378. https://doi.org/10.1109/JSYST.2021.3123904

Pourbeik, P., Kundur, P. S., & Taylor, C. W. (2006). The anatomy of a power grid blackout—Root causes and dynamics of recent major blackouts. *IEEE Power and Energy Magazine*, *4*(5), 22–29. https://doi.org/10.1109/MPAE.2006.1687814

Rampurkar, V., Pentayya, P., Mangalvedekar, H. A., & Kazi, F. (2016). Cascading Failure Analysis for Indian Power Grid. *IEEE Transactions on Smart Grid*, *7*(4), 1951–1960. https://doi.org/10.1109/TSG.2016.2530679

Ross, R., Graubart, R., Bodeau, D., & McQuaid, R. (2018). *Systems Security Engineering: Cyber Resiliency Considerations for the Engineering of Trustworthy Secure Systems* (NIST Special Publication (SP) 800-160 Vol. 2 (Withdrawn)). National Institute of Standards and Technology. https://csrc.nist.gov/Pubs/sp/800/160/v2/IPD

Rueda, J. L., Cepeda, J. C., Erlich, I., Korai, A. W., & Gonzalez-Longatt, F. M. (2014). Probabilistic Approach for Risk Evaluation of Oscillatory Stability in Power Systems. In F. M. Gonzalez-Longatt & J. Luis Rueda (Eds.), *PowerFactory Applications for Power System Analysis* (pp. 249–266). Springer International Publishing. https://doi.org/10.1007/978-3-319-12958-7_11

Rzysztof, & Roka. (2019). *The risk of large blackout failures in power systems*. https://www.semanticscholar.org/paper/The-risk-of-large-blackout-failures-in-power-Rzysztof-Roka/31e364486ab57008bfb9a938eed2d311392366a5

Sabeeh, B., & Gan, C. (2016). *Power System Frequency Stability and Control: Survey*. *11*, 5688–5695.

Sanjeev, P., Padhy, N. P., & Agarwal, P. (2018). Peak Energy Management Using Renewable Integrated DC Microgrid. *IEEE Transactions on Smart Grid*, *9*(5), 4906–4917. https://doi.org/10.1109/TSG.2017.2675917

Shair, J., Li, H., Hu, J., & Xie, X. (2021). Power system stability issues, classifications and research prospects in the context of high-penetration of renewables and power electronics. *Renewable and Sustainable Energy Reviews*, *145*, 111111. https://doi.org/10.1016/j.rser.2021.111111

Sharma, N., Acharya, A., Jacob, I., Yamujala, S., Gupta, V., & Bhakar, R. (2021). Major Blackouts of the Decade: Underlying Causes, Recommendations and Arising Challenges. *2021 9th IEEE International Conference on Power Systems (ICPS)*, 1–6. https://doi.org/10.1109/ICPS52420.2021.9670166

Shazon, Md. N. H., Nahid-Al-Masood, & Jawad, A. (2022). Frequency control challenges and potential countermeasures in future low-inertia power systems: A review. *Energy Reports*, *8*, 6191–6219. https://doi.org/10.1016/j.egyr.2022.04.063

Shekari, T., Cardenas, A. A., & Beyah, R. (2022). MaDIoT 2.0: Modern High-Wattage IoT Botnet Attacks and Defenses. *31st USENIX Security Symposium (USENIX Security 22)*, 3539–3556.

Soltan, S., Mittal, P., & Poor, H. V. (2018). BlackIoT: IoT botnet of high wattage devices can disrupt the power grid. *27th USENIX Security Symposium (USENIX Security 18)*, 15–32.

Song, J., Cotilla-Sanchez, E., Ghanavati, G., & Hines, P. D. H. (2016). Dynamic Modeling of Cascading Failure in Power Systems. *IEEE Transactions on Power Systems*, *31*(3), 2085–2095. https://doi.org/10.1109/TPWRS.2015.2439237

Staid, A. (2021). *North American Energy Resilience Model (NAERM)*.

Stouffer, K., Lightman, S., Pillitteri, V., Abrams, M., & Hahn, A. (2014). NIST special publication 800-82, revision 2: Guide to industrial control systems (ICS) security. *National Institute of Standards and Technology*.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., & Lightman, S. (2022). *Guide to Operational Technology (OT) Security: Initial Public Draft* [Preprint]. https://doi.org/10.6028/NIST.SP.800-82r3.ipd

Sun, C.-C., Hahn, A., & Liu, C.-C. (2018). Cyber security of a power grid: State-of-the-art. *International Journal of Electrical Power & Energy Systems*, *99*, 45–56. https://doi.org/10.1016/j.ijepes.2017.12.020

Taurins, E. (2020). *How to set up CSIRT and SOC* [Report/Study]. ENISA. https://www.enisa.europa.eu/publications/how-to-set-up-csirt-and-soc

UCTE. (2006). *Final Report System Disturbance on 4 November 2006*.

Union, P. O. of the E. (2016, April 14). *Commission Regulation (EU) 2016/631 of 14 April 2016 establishing a network code on requirements for grid connection of generators (Text with EEA relevance), C/2016/2001* [Website]. Publications Office of the EU; Publications Office of the European Union. https://op.europa.eu/en/publication-detail/-/publication/1267e3d1-0c3f-11e6-ba9a-01aa75ed71a1/language-en

Vaz, R. (2020). Venezuela's power grid disabled by cyber attack. *Green Left Weekly*, *1213*, 15. https://doi.org/10.3316/informit.254960650542537

Vellaithurai, C., Srivastava, A., Zonouz, S., & Berthier, R. (2015). CPIndex: Cyber-Physical Vulnerability Assessment for Power-Grid Infrastructures. *IEEE Transactions on Smart Grid*, *6*(2), 566–575. https://doi.org/10.1109/TSG.2014.2372315

Wang, Y., Chen, C., Wang, J., & Baldick, R. (2016). Research on Resilience of Power Systems Under Natural Disasters—A Review. *IEEE Transactions on Power Systems*, *31*(2), 1604–1613. https://doi.org/10.1109/TPWRS.2015.2429656

Wilson, E., Conneely, T. M., Mudrov, A., & Tyukin, I. (2019). Implementation of the Prony Method for Signal Deconvolution. *IFAC-PapersOnLine*, *52*(29), 269–273. https://doi.org/10.1016/j.ifacol.2019.12.661

Xiong, L., Liu, X., Liu, Y., & Zhuo, F. (2022). Modeling and Stability Issues of Voltage-source Converter-dominated Power Systems: A Review. *CSEE Journal of Power and Energy Systems*, *8*(6), 1530–1549. https://doi.org/10.17775/CSEEJPES.2020.03590

Xiong, W., Wang, L., Wu, R., Qi, Y., Liu, H., & Bi, T. (2020). Decision Tree Based Subsynchronous Oscillation Detection and Alarm Method Using Phasor Measurement Units. *2020 IEEE Sustainable Power and Energy Conference (ISPEC)*, 2448–2453. https://doi.org/10.1109/iSPEC50848.2020.9351274

Zhao, J., Wang, J., & Yin, L. (2016). Detection and Control against Replay Attacks in Smart Grid. *2016 12th International Conference on Computational Intelligence and Security (CIS)*, 624–627. https://doi.org/10.1109/CIS.2016.0151

Annexes

1 Annex I: EPES asset characterization

For the resilience mitigation actions definition, the starting point is the classification of the energy sector asset and associated threats. Once assets and threats are enumerated, the dynamic risk assessment process can be conducted, and its outputs can be used for the definition of the resilience mitigation actions to increase EPES resilience considering the real EPES vulnerabilities.

The electrical grids provide electricity from its generation to the customers and it consists mainly in a complex interconnection between generation, transmission, distribution, and end-users. The generated power is transferred through the transmission lines to the distribution lines. This transferred power is distributed through the distribution lines to the consumers reducing the voltage to a desirable level to be used by consumers.

The key supply chain components of electric grids are power generators, electricity transmission and distribution networks, and end-users.

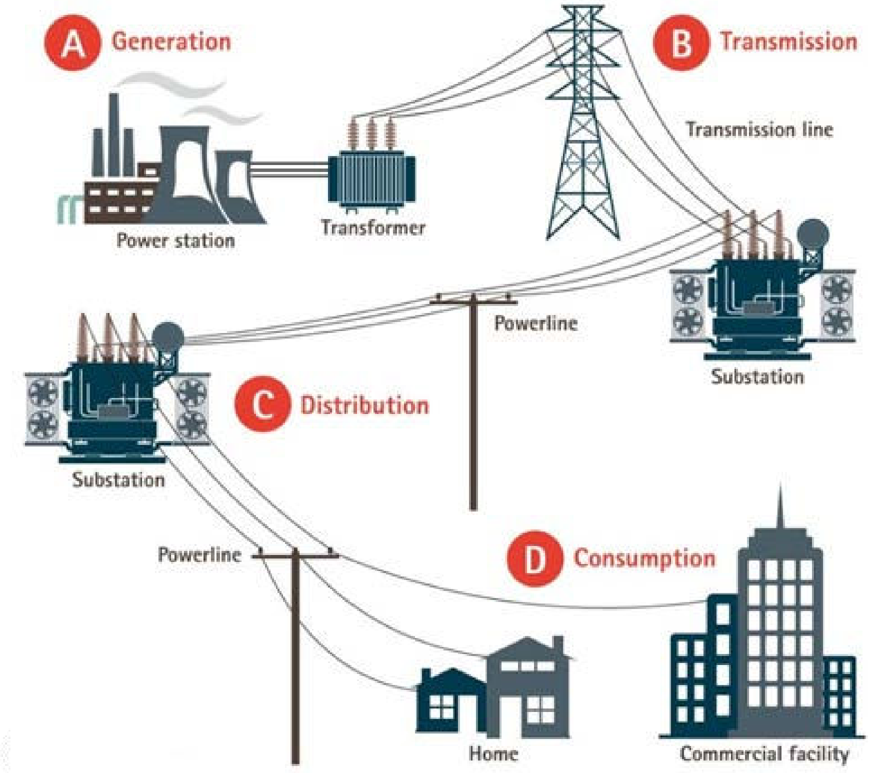


Figure 23. Electric grid main components

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

1.1 Power generators

The traditional electricity generation source has been fossil-fuel power plants, but the fraction of electric power produced from these traditional power plants has decreased in favour of Renewable Energy Sources (RES). The RES from 2005 until today has more than doubled, as reported by European Environment Agency. The electrification of transport is a clear example of the electricity generation transformation from conventional power plants to renewable generation.

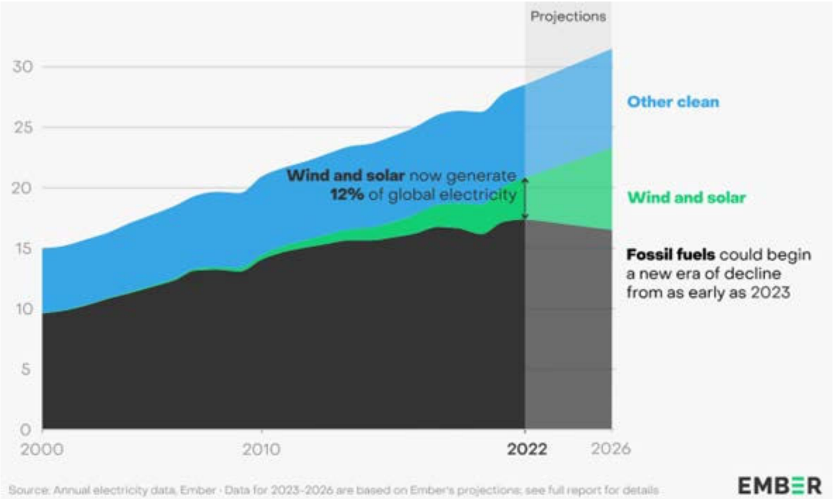


Figure 24. Replication of traditional power plants (Ember's analysis, 2022, p. 20)

The main assets composing the generation plants can be identified by: primary fuel; *solar panels, solar thermal collectors, Inverters; wind turbines; pumps; motors; valves; pipelines; electricity generators; condensers; nuclear reactors,* etc. For the definition and distinction of the resilience mitigation actions, the power plant types, and associated asset types are considered.

1.2 Electricity transmission and distribution networks

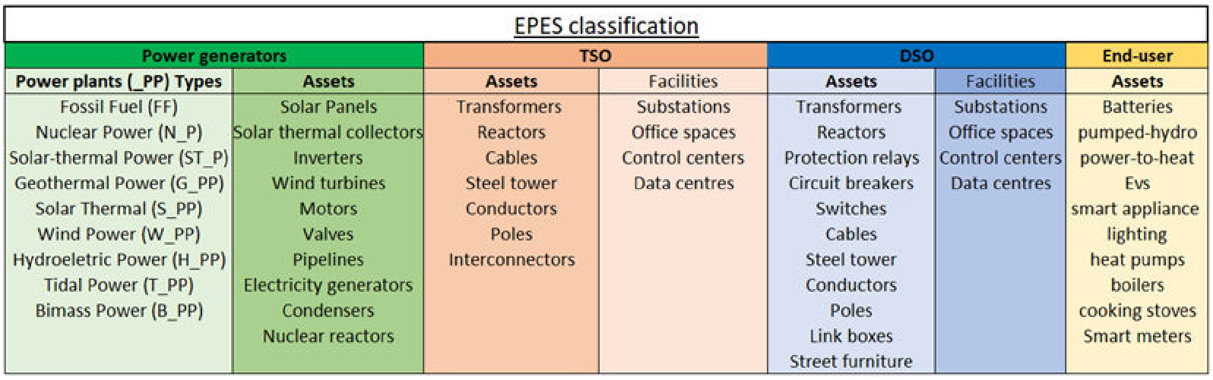
The electricity transmission networks are used to transfer the power generated by the power plants to the distribution lines by increasing the voltage to decrease the resistance in the lines and reduce losses. The Transmission System Operators (TSO) are responsible for the operation, maintenance, and development of the transmission networks. TSOs' responsibility is also to ensure the stability of the electricity grid by maintaining a constant balance between demand and supply to avoid frequency disparities or supply disruption. The main assets of transmission systems are *transmission substation assets such as transformers and reactors; transmission circuit assets such as cables, overhead lines, and poles; Interconnectors*. Part of the transmission system are also facilities, including substations, office spaces, control centres, etc.

The electricity distribution networks are used to deliver the generated power from the transmission lines to the consumers. In order to satisfy the desirable voltage needed by the consumers, the distribution lines step down the voltage before it reaches the end customers through different electric substations. The electricity passes from High

Voltage (HV) to Medium Voltage (MV) or Low Voltage (LV). Typically, the end-user can be divided into industrial, commercial, and residential. The main assets of *distribution* systems are *distribution substation assets such as transformers and reactors.* Part of the distribution system are also facilities, including substations, office spaces, control centres, etc.

1.3 End-users / customers

This last component includes stationary devices, electric vehicles, and domestic loads such as appliances, lighting, heat pumps, boilers, etc.



EPES classification

Power generators		TSO		DSO		End-user
Power plants (_PP) Types	**Assets**	**Assets**	Facilities	**Assets**	Facilities	**Assets**
Fossil Fuel (FF)	Solar Panels	Transformers	Substations	Transformers	Substations	Batteries
Nuclear Power (N_P)	Solar thermal collectors	Reactors	Office spaces	Reactors	Office spaces	pumped-hydro
Solar-thermal Power (ST_P)	Inverters	Cables	Control centers	Protection relays	Control centers	power-to-heat
Geothermal Power (G_PP)	Wind turbines	Steel tower	Data centres	Circuit breakers	Data centres	Evs
Solar Thermal (S_PP)	Motors	Conductors		Switches		smart appliance
Wind Power (W_PP)	Valves	Poles		Cables		lighting
Hydroeletric Power (H_PP)	Pipelines	Interconnectors		Steel tower		heat pumps
Tidal Power (T_PP)	Electricity generators			Conductors		boilers
Bimass Power (B_PP)	Condensers			Poles		cooking stoves
	Nuclear reactors			Link boxes		Smart meters
				Street furniture		

Figure 25. EPES classification

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

2 Annex II: Analysis of cascading failures

2.1 Historical analysis of blackouts

Below is a review of some of the major cascading failures and power grid blackouts that have occurred around the globe since the year 2000:

- U.S.-Canadian blackout on 14th August 2003:

According to the North American Electric Reliability Corporation (NERC) report on this blackout (Eto, 2004), the blackout started just after 4 p.m. EDT time. Before the tripping of the first line, the system was liable to more than 800 contingencies based on the steady-state (power flow) analysis. From the pre-condition perspective, based on this report, the network was on peak load. Besides, some events could have adversely affected the system, like low voltage in the Cleveland-Akron area, warm weather in the Midwest and Northeast, high interregional power transfers, unavailability of specific generators or transmission lines, and frequency anomalies. These pre-conditions somehow put the system under instability stress. However, two of the most influential events in this blackout were the failure of the alarm and logging system in the FirstEnergy electric utility control room, which was not restored until after the blackout, and the Midwest Independent System Operator (MISO) state estimation malfunction. Since the operators were unaware of a major system problem, the occurrence of two faults due to tree contacts shifted power flows on other lines and caused the tripping of several lines. Based on (Eto, 2004), because of a lack of sufficient awareness of FirstEnergy, they did not perform sufficient load-shedding, and the outage spread throughout the system. A general overview of the U.S.-Canadian 2003 blackout is provided in Figure 26 from pre-condition to the blackout.

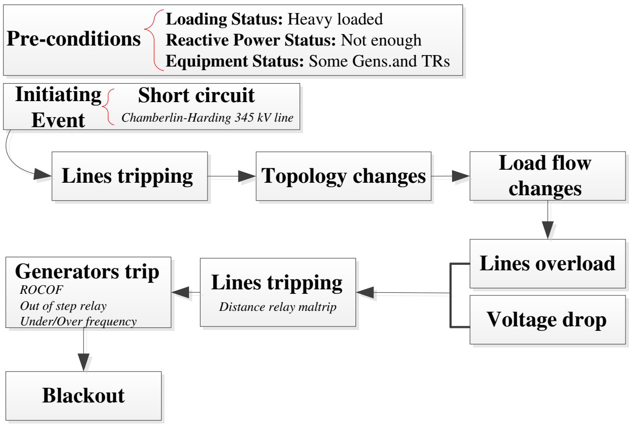


Figure 26. U.S.-Canadian 2003 blackout mechanism

- Italian Blackout, 2003

On September 28th, 2003, Italy experienced a widespread blackout that affected almost the entire country. The blackout started with a tree in Switzerland bringing down a high-voltage power line. This led to a cascading failure, which ended up affecting the power

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

grid in Italy. In the incident, a tree flashover caused the tripping of a major tie-line between Italy and Switzerland. The Italian system lost synchronism with other parts of Europe, and a cascade tripping of 16 transmission lines to Italy was recorded. This left the Italian power system with a deficit of almost 6400 MW, leading to the total collapse of the Italian power system. The blackout lasted several hours in the different Italian regions, as shown in the next figure, and affected 56 million people (Corsi & Sabelli, 2004). The total service interruption duration was 3 hours in the north, 9 hours in the centre, 12 hours in the south, and 16 hours in Sicily.

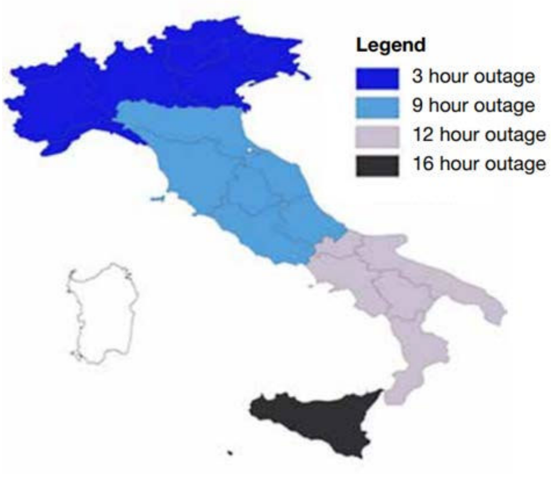


Figure 27. Power outage in Italy (2003)

The economic losses and effects due to this power outage are presented in the next table. The damage to businesses is calculated at 897.5 million € (*OSCE Organization for Security and Co-operation in Europe*).

Table 4. Power outage (Italy) – Economic Losses [Million euro]

Location	**Primary sector**	**Secondary sector**	**Tertiary sector**	**Total Losses**	**WTP Households**	**Total Losses in the Region**
North	5.3	136.7	60.8	202.8	43.0	**245.8**
Center	20.6	217.6	154.6	392.8	98.2	**491.0**
South	20.9	82.8	97.5	201.2	94.3	**295.5**
Sicily	12.4	33.7	54.6	100.7	49.5	**150.2**
Total	59.2	470.8	367.5	897.5	285.0	**1182.5**
% of GDP	0.004%	0.031%	0.025%	0.060%	0.019%	**0.079%**

- Swedish-Danish Blackout, 2003

On September 23th, 2003, a blackout occurred in the Swedish/Danish system due to a series of equipment failures and maintenance issues. Initially, a 1200 MW nuclear unit in southern Sweden tripped, followed by a double bus bar fault at one of the substations. The only remaining line, a 400 kV transmission line, failed under heavy load and caused

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

system separation due to voltage collapse. This blackout affected almost 4 million customers.

- Indian blackout on 30th July 2012:

The power outage in India on July 30th and 31st, 2012, was one of the most significant blackouts in history, affecting an estimated 600 million people and accounting for 9 percent of the world's population (Rampurkar et al., 2016). According to the report by the Central Electricity Regulatory Commission (Rampurkar et al., 2016), before the initiation of a sequence of failures, the northern region of the Indian grid was in high-load condition, which was fed by the west and east regions. Moreover, some transmission lines were under outage prior to the occurrence of the disturbance. The reasons for the outage of the transmission lines are classified as planned outages, forced outages, and lines opened to control high voltages in the system. The cascading failures started with the outage of two 400 kV tie lines between the north and west regions which overloaded other tie lines. After this, cascading failures were initiated, and a sequence of events occurred, leading to the Northern Region's separation from the whole grid. Subsequently, although the Under Frequency Load Shedding scheme (UFLS) and Rate of Change of Frequency (ROCOF) relays operated due to load generation imbalance in the Northern Region, sufficient loads were not shed, and Northern Region collapsed. The rest of the Indian grid also collapsed due to excess generation.

- South Australian Blackout, 2016

This was a statewide blackout occurring in September 2016, affecting South Australia. The blackout resulted from severe storm conditions, which led to the cascading tripping of the power line and wind farms. The event highlighted the challenges of integrating renewable energy into the grid and led to a nationwide debate about the reliability of renewable energy.

- Brazilian Blackout, 2018

On March 21, 2018, a power outage struck the Brazilian power system due to a failure of a transmission line near the Belo Monte hydropower station. About 18,000 MW of power was curtailed during this disturbance, affecting more than 10 million customers. This incident led to recommendations on enhancing the system against major disturbances as well as improving the black-start restoration capabilities.

- California Rolling Blackouts, 2020-2021

In response to extreme heatwaves and high demand for electricity, California's grid operator initiated the first rolling blackouts since the 2001 energy crisis. The blackouts affected hundreds of thousands of people and sparked a renewed debate about the state's shift towards renewable energy and the reliability of the grid. The grid was not prepared for the surge in demand, leading to supply shortages.

- Texas Blackout, 2021

This blackout occurred due to a severe winter storm that led to a sudden drop in temperature, affecting natural gas production and freezing wind turbines. This, combined with a spike in electricity demand due to heating needs, caused a failure in the state's power grid. The grid was unable to handle the stress due to several issues, including inadequate weatherization of power infrastructure and lack of preparation for such extreme weather events. Millions of people were left without power for several days.

- Continental Europe cascading failures on 8th January 2021:

On Friday, 8th January 2021, at 2:05 PM Central European Time, the Central Europe synchronous area was split into two distinct regions (the northwest and the southeast regions) due to multiple transmission network cascading failures. However, this series of events did not lead to the power system blackout and just divided Central Europe Power System into two asynchronous areas. Before the incident, the system was heavily loaded, and the northwest region had a power shortage of 5.8 GW, while the southeast region had an excess of power. Moreover, there were some planned outages the day before the incident, including the 400 kV Ernestinovo (HR) – Pecs (HU) line was out of service due to a technical circuit breaker failure, 400 kV Žerjavinec (HR)–Heviz (HU) line was out of service due to corrective measure for voltage reduction. The trip on the busbar coupler in the Croatian substation Ernestinovo instigated the cascading failures. Subsequently, according to the load pattern from South-East to North-West Europe, which accounts for 5.8 GW, the substation experienced high-load flow. At the moment, the security calculations were not estimated for high-load flow, especially on the busbar coupler, and before the initial incident occurred, the power system was already in the angular instability limit. As a result of the significant frequency variations in both regions, automatic reserves that control frequency were activated soon after the system split and helped stabilize the frequency quickly. This stabilization was also achieved by the implementation of additional frequency support measures, such as the use of automatic loads that can be interrupted in France and Italy, as well as through high-voltage direct current lines from power systems in the Nordic countries and Great Britain. Finally, the resynchronization process was done after 1 hour.

These blackouts underscore the importance of robust and resilient grid infrastructures, which include enhanced real-time monitoring, better coordination between grid operators, and the adoption of advanced technologies to increase the flexibility and reliability of the power grid.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Table 5. Pre-conditions for major historical blackouts around the world

Location	Date	Pre-condition				
		Loading	**Equipment status**	**Dependency among regions**	**Inadequate reactive power reserves**	**PF mismatch & lack of awareness**
Brazil	4th February 2011	Normal load	500kV transmission line was out of service	P	-	-
USA/Mexico	8th September 2011	Normal load	Several generators and two lines were out of service	-	-	P
Chile	24th September 2011	Normal load	Five transmission lines were out of service	P	-	-
India	30th-31st July 2012	Peak load	Several generators and transmission lines were out of service	P	P	P
Turkey	31st March 2015	Normal load	400kV line out of service	P	P	
Bangladesh	1st November 2014	Off-peak	Some generators were under maintenance	Roughly 10% of power was imported from the HVDC line connected to India (small inertia)	-	-
Pacific Southwest	8th September 2011	Peak load	some generation and transmission lines were under maintenance outages	Arizona, Southern California, and Baja California, Mexico, with heavy power imports into Southern California from Arizona.	P	-
Turkey	31st March 2015 (spring)	Off-peak	Four important 400 kV lines and all (16) series capacitor (SC) banks were out of service.	East to the West of Turkey	-	No adequate awareness about the importance of the series

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Location	Date	Pre-condition				
		Loading	Equipment status	Dependency among regions	Inadequate reactive power reserves	PF mismatch & lack of awareness
						capacitors for angular stability
Italy	28th September 2003	The whole Italian was close to its minimum. But, the northwest border of Italy was highly loaded	Some of the most important Italian power stations were offline for economic reasons, and Two transmission lines were out of service.	The most important interconnection lines are those to the French (three 380 kV and one 220 kV lines) and the Swiss (two 380 kV and six 220 kV lines) systems.	-	-
U.S.-Canadian blackout	14th August 2003	Peak load	Some generation and transmission lines were under maintenance outages	P	reactive power supply problems	P
Swedish/Danish	23rd September 2003	Normal load	two 400-kV lines and HVDC links connecting the Nordel system with continental Europe were out of service due to maintenance.	P	-	-
Croatia and Bosnia Herzegovina	12th January 2003	Peak load	Seven transmission lines were out of service.	P		
Athens Blackout	12th July 2004	The system (especially during Summer) is prone to voltage instability.	One 125 MW generating unit and one generating unit in Northern Greece were out of service.	power transfer from the generating areas in the North and West of Greece to the main load center in the Athens metropolitan area		

Table 6. Initiating events for major historical blackouts around the world

Location	Date	Initial events			
		SC	**Overload**	**Hidden failure**	**Others**
Indonesia	2005/08/18			P	
Colombia	2007/04/26		P		
Brazil	2009/11/10	P			
Brazil	2011/02/04			P	
Chile	2011/09/24	P			
India	2012/07/30-31		P		
Turkey	2015/03/31		P	Although the Turkish 400 kV grid is equipped with a protection system that is in line with international standards, the effect of the distance relay settings on the line that tripped first was not correctly evaluated.	
Australia	2016/09/28	P			
Greek (Kefallonia Island)	2006/01/24	P Bad weather			
Vietnam	22nd May 2013	PTree fell			
Pacific Southwest	8th September 2011	P		P	
Italy	September 28th, 2003	flashover towards a tree		Lacking a sense of urgency regarding the San Bernardino (SILS-SOAZZA) line overload	

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Location	Date	Initial events			
		SC	**Overload**	**Hidden failure**	**Others**
				and call for inadequate countermeasures in Italy	
U.S.-Canadian blackout	14th August 2003				Due to high reactive output, the Eastlake Unit 5 voltage regulator tripped to manual due to overexcitation.
Swedish/Danish	23rd September 2003				1,200-MW nuclear unit in southern Sweden tripped due to problems with a steam valve.
Croatia and Bosnia Herzegovina	12th January 2003	short circuit on OHL 400 kV Konjsko - Velebit near bus Velebit is recognized as the triggering event		Protection mal-function	

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

2.2 Role of power system stability in cascading failures

Rotor angle stability is a critical aspect of stability in cascading failures and refers to the capability of synchronous machines in interconnected power systems to recover to synchronism after being subjected to a disturbance (Kundur et al., 2004). Instability in rotor angle can result in increasing angular swings, leading to a loss of synchronism. The synchronism of a machine relies on the balance between electromagnetic torque and mechanical torque delivered by the prime mover. Insufficient or negative synchronizing torque can cause aperiodic or non-oscillatory transient instability with large rotor angle excursions. Conversely, the lack of negative damping torque can lead to small-disturbance oscillatory stability, including local plant mode oscillations and interarea mode oscillations.

During a short circuit, the transient stability of the power system is directly affected as the rotor angles of machines deviate. If protection schemes are appropriately designed, distance relays will trip the line with the fault, and the system will return to normal conditions. However, if the fault is not cleared promptly, the angular separation will increase, reaching a point where the out-of-step protection of the generator trips the synchronous machine to prevent physical damage. Additionally, interarea oscillations in interconnected power grids can cause component outages if they are not effectively damped. Based on these interpretations, it can be concluded that rotor angle stability plays a crucial role in the system's dynamic response following short circuits. If the system fails to respond to disturbances, it can lead to component outages and trigger a chain of cascading events by reducing the security margin in system operation.

Analyzing voltage stability is also crucial to understand the propagation of cascading failures. Voltage stability refers to the ability of a power system to maintain steady voltages at all buses in the system after being subjected to a disturbance from a given initial operating condition. In other words, voltage stability relates to the system’s ability to restore equilibrium between load and supply. Voltage instability may result in progressive voltage fall or rise in certain buses, leading to tripping transmission lines or load loss in specific areas. Furthermore, a chain of failures accompanied by voltage instability can cause voltage collapse and result in a blackout. Reactive power flow is a critical factor associated with voltage stability as it directly influences bus voltage magnitudes. The capacity of the transmission network plays a key role in maintaining the voltage profile in power systems. For example, when a transmission line is out for maintenance, it limits the power system's capability to transfer power, leading to voltage stability issues in certain regions. The time frame for voltage stability problems can vary from a few seconds to tens of minutes. Therefore, voltage stability contributes to the pre-condition and initiation of cascading failures and is a determining factor in both slow and fast cascading events.

This project has received funding from the European Union’s
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

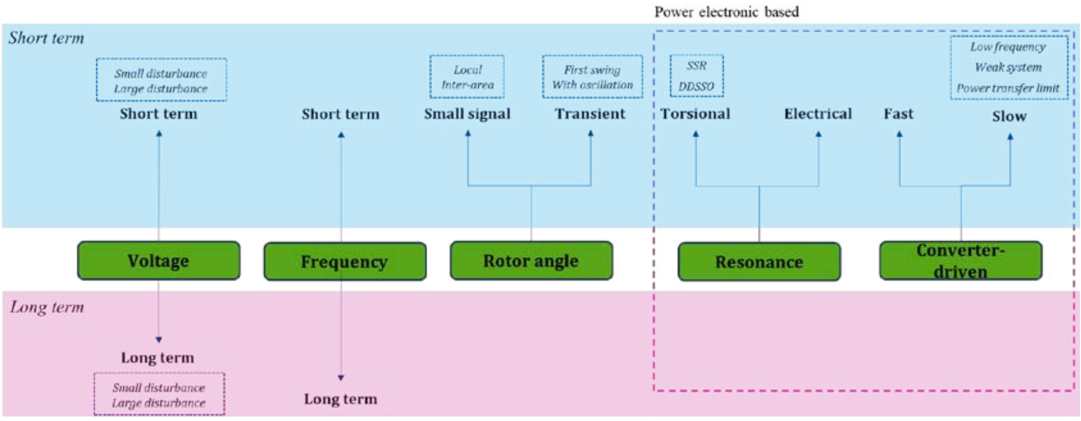


Figure 28. Revised classification of stability in the power system

In an interconnected power system dominated by synchronous generation, system frequency control, and stability are paramount. Sudden changes in load or generation can cause imbalances, resulting in frequency excursions in the power system. The response to this divergence and frequency recovery process involves three essential stages in power systems: initial inertial response, primary frequency response (turbine-governor droop response), and automatic generation control (secondary control) (Sabeeh & Gan, 2016). Initially, all generators' rotational inertia responds to the disturbance based on physical principles. Depending on the imbalance between load and generation, synchronous machines may slow down or speed up, resulting in frequency excursions. The primary frequency response aims to maintain frequency stability through turbine-governor control. If this control is insufficient to restore the frequency to its normal value, automatic generation control acts as the third stage to recover the frequency and eliminate frequency deviations. The effectiveness of automatic generation control depends on the reserve capacity of the system. If these controls fail to preserve frequency stability, load-shedding relays are activated to restore frequency and balance between load and generation. The system's frequency response is a dominant factor in the underlying mechanism of cascading failure propagation, especially in the fast-cascading stage. A sudden increase in load or loss of generation can cause a significant frequency drop. If the power system lacks adequate active power spinning reserve, this rapid frequency decline can lead to under-frequency conditions, triggering generator tripping through ROCOF or under-frequency protection. Furthermore, long-term frequency stability can contribute to pre-conditioning or slow cascading failures when the power system cannot provide sufficient frequency recovery reserve after disturbances.

With the significant integration of renewable energy resources, energy storage, and fast-response power electronic devices, the dynamic response of power systems has become more reliant on these technologies (Hatziargyriou et al., 2021). Power electronic converters, in particular, have reduced the system's inertial response to faults, making it more vulnerable to large disturbances. Additionally, the complex control loops of these devices introduce new stability and resonance issues in power systems. However, advanced power electronic converters can contribute to frequency and voltage control and provide virtual inertia to power systems(Shair et al., 2021). Figure 28 illustrates the extended version of the classification of power system stability to address this issue.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

Based on the revised classification, resonance and convert-driven stability also play a major role in the system’s dynamic response.

Resonance stability focuses on torsional and electrical resonance within power systems, while converter-driven stability can be categorized as slow interaction and fast interaction. Fast interaction pertains to the rapid dynamics of power electronics converter control loops and can lead to stability issues such as harmonic instability and multi-resonance peaks. Slow interaction-based stability relates to the interaction of converters with the slow dynamics of power systems, such as the electromechanical response of synchronous machines.

Torsional resonance originated from interactions between the series compensated line(s) and the turbine-generator mechanical shaft (Hatziargyriou et al., 2020). In contrast, the electrical resonance is mostly caused by the inherent negative resistance of the induction generator rotor. The self-excitation Sub-Synchronous Resonance (SSR) was observed for the first time in the field by the Electric Reliability Council of Texas (ERCOT) in 2009 (Cheng et al., 2016). Similar events, including Doubly-Fed Induction Generators (DFIG) and series compensation, have been observed in the Xcel Energy network in Minnesota (Narendra et al., 2011).

Convert-driven stability can be divided into slow and fast interactions. The fast interaction is mainly concerned with the rapid dynamic of the control loop of power electronics converters. These fast interactions can cause several stability issues, such as harmonic instability and multi-resonance peaks. However, the slow interaction-based stability is related to converters' interaction with power systems' slow dynamics.

2.3 Mechanism of blackouts

This section examines the historical blackouts combined with pre-condition, the initiating event, power system stability, and protection to obtain a generic scenario of cascading failures and blackouts. According to the historical blackouts, several phenomena are behind system response during cascading failures. These phenomena are highly nonlinear and complex because of the system's complexity and interdependency. Typically, the five most critical types of phenomena have a higher contribution to the propagation of cascading failures: (i) loss of synchronism, (ii) voltage instability, (iii) generator over excitation & loss of excitation, (iv) system response, and (v) frequency instability. It is worth noting that other phenomena like resonance can also occur during cascading failures, but the likelihood of these events happening is relatively low. This section analyzes each of these phenomena considering pre-condition and initiating events. In the following, the concept of "Building Blocks (BB)" refers to the phenomena contributing to cascading failure propagation.

a) BB1: Loss of synchronism

As discussed, one of the critical aspects of power system stability is loss of synchronism, which refers to the ability of generators to maintain their synchronous operation. Loss of synchronism occurs when the relative rotor angles of interconnected generators deviate significantly from their nominal values, leading to a loss of system stability. This deviation can arise due to pre-conditions and faults that disrupt the balance between generation

This project has received funding from the European Union’s Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

and demand. More specifically, an outage of a transmission line, either a planned outage for maintenance or a fault, can affect the rotor angle stability margin. Figure 29 shows the BB1 related to loss of synchronism. According to this BB1, a transmission line outage changes the system's topology. This may increase the system's path reactance, as indicated in Figure 30. Figure 31 shows a P-δ curve related to the generator rotor angle stability. As shown in this figure, by changing the topology and increasing the path reactance, based on (1), the P_{max}, the maximum power a generator can provide, is decreased. Hence reduces the rotor angle stability margin and makes the system more vulnerable to further line failures.

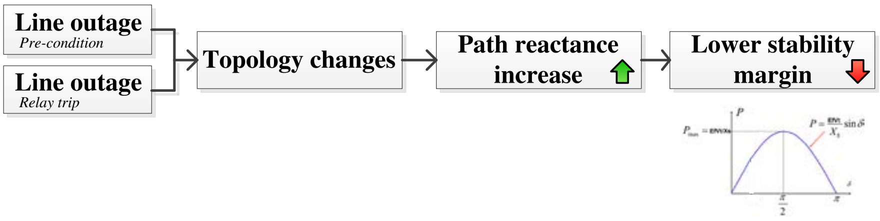


Figure 29. BB1: loss of synchronism

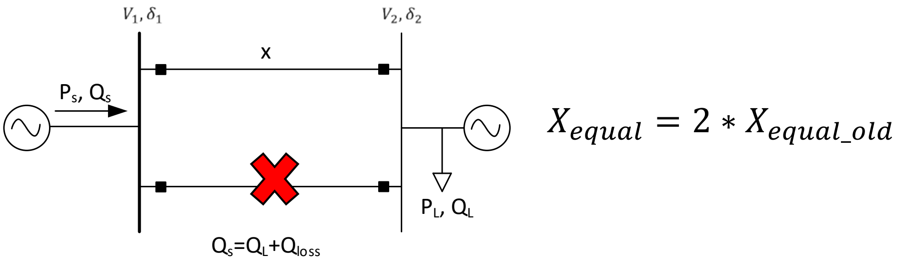


Figure 30. Equivalent path reactance after an outage

$$P_e = \frac{V_1 \times V_2}{X} \sin\delta \qquad (1)$$

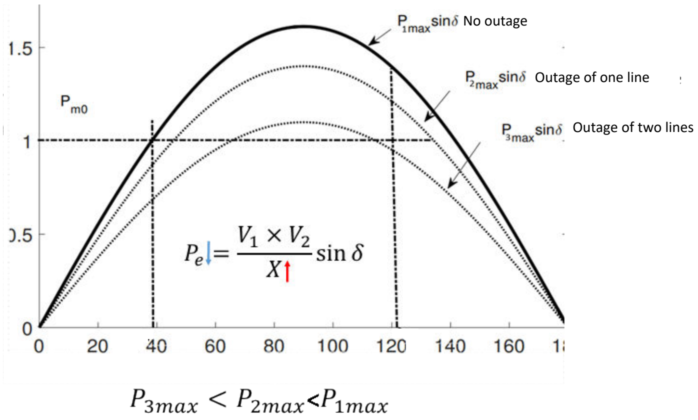


Figure 31. P-δ curve - generators rotor angle stability

In summary, an outage due to pre-conditions or an initiating event not only jeopardizes the rotor angle stability but can also reduce the system's ability to respond to further disturbances by decreasing the rotor angle stability margin.

b) BB2: Voltage instability

Voltage instability is another critical aspect of power system stability that contributes to cascading failures and blackouts. In this section, the dependencies of voltage instability, pre-conditions, initiating events, and protection schemes are explored to shed light on the mechanisms that trigger and propagate cascading failures. The schematic diagram of BB2 is depicted in Figure 32. According to this figure and as discussed in the previous section, an outage of a transmission line due to pre-conditions or initiating events can change the grid's topology. The outage of a transmission line causes the power flow re-dispatch, and consequently, the line currents increase. On the other hand, by changing the topology, the overall path reactance of the system increases. Combining these two, active and reactive transmission line losses increase. Hence, a high reactive power demand issue appears in the power system. To solve this issue, generators typically increase their reactive power generation. Despite attempts to address the issue, an increase in reactive power generation results in higher losses and reactive power deficiency. As a result of the high reactive power demand issue, the voltage drops, which causes a cascading overload of the lines and transformers.

In summary, the interdependencies between pre-conditions, high reactive power demand, and voltage instability highlight the importance of addressing these factors to mitigate cascading failures. Prompt recognition of pre-conditions and proactive measures to maintain an adequate reserve margin of reactive power is vital for preventing voltage instability.

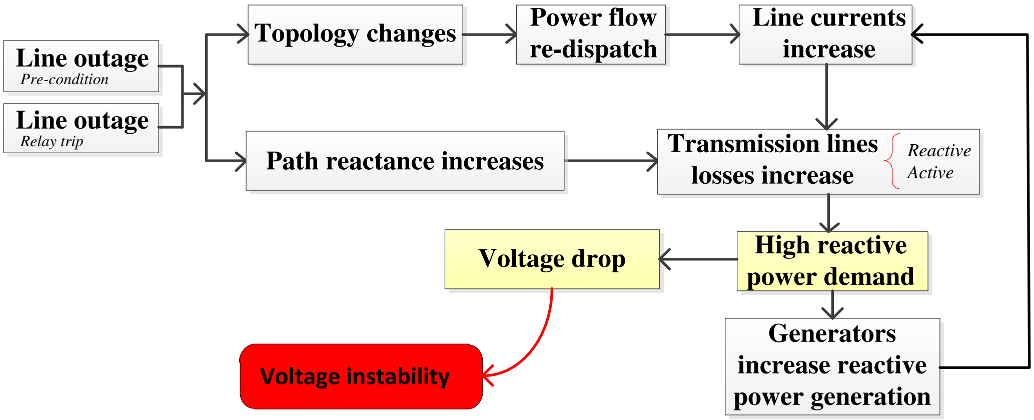


Figure 32. BB2: voltage instability and high reactive power demand

c) BB3: Generator over excitation and loss of excitation

In power systems, generators maintain voltage stability and provide reactive power support to meet the network's demand. However, under certain pre-conditions and initiating events, generators can experience over-excitation or loss of excitation, leading to adverse effects on system stability and cascading failures. One of the conditions that can contribute to generators' over-excitation and loss of excitation is the outage of a transmission line (Figure 33). The loss of a transmission line alters the network's topology and can result in changes to the reactive power flow patterns, whether due to the planned maintenance or a fault condition. This change in power flow distribution can lead to an increased demand for reactive power in specific areas of the network. In this regard, in response to the increased reactive power demand, generators attempt to generate additional reactive power to maintain voltage stability. This adjustment is achieved by increasing the excitation system's output and field current. However, if the reactive power demand exceeds the generator's capability, the excitation system can become overburdened, resulting in over-excitation. Over-excitation occurs when the generator's terminal voltage exceeds its normal operating range, jeopardizing the stability and performance of the generator.

Conversely, when the fault is near the generator, and the reactive power demand is excessive, the generator's field current drops below the level required to maintain its rated voltage, leading to a significant decrease in voltage magnitude and compromising the generator's ability to contribute to system stability. As a result, the generator can experience a loss of excitation, and the generator's excitation system fails to supply sufficient reactive power. Generators' over-excitation or loss of excitation can have cascading effects on the power system, exacerbating the vulnerabilities introduced by the initiating event.

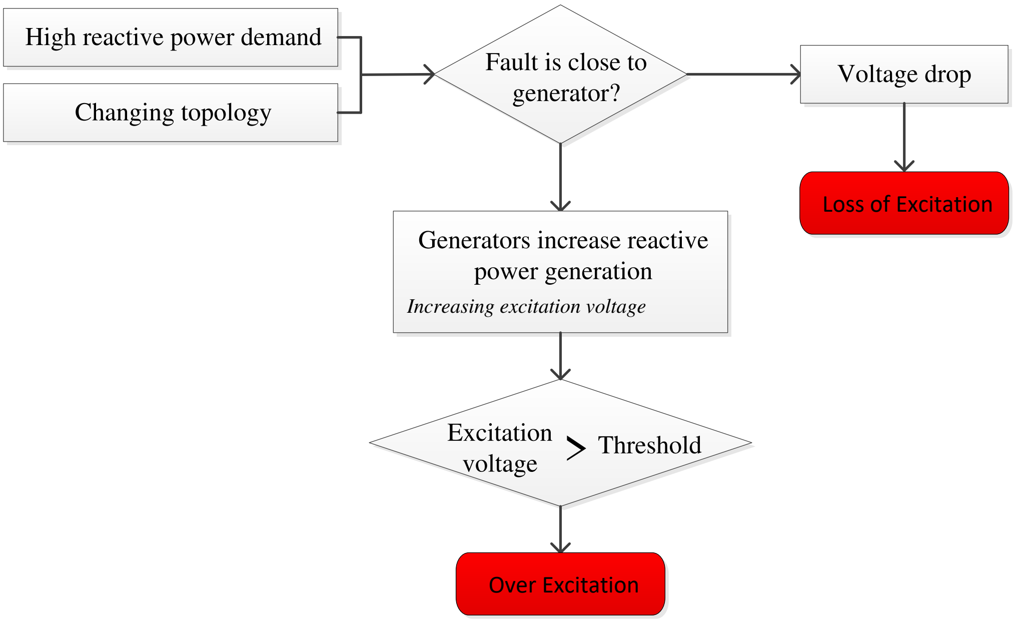

High reactive power demand
Changing topology
Fault is close to generator?
Voltage drop
Loss of Excitation
Generators increase reactive power generation
Increasing excitation voltage
Excitation voltage > Threshold
Over Excitation

Figure 33. BB3: Generators over-excitation or loss of excitation

d) BB4: System response

The power system's response to pre-conditions and initiating events play a vital role in determining the stability and resilience of the network. In the context of power systems, system response refers to how the network reacts and adapts to changes in operating conditions, disturbances, or events. It involves the dynamic behavior of various components, such as generators, transmission lines, transformers, and loads, as they respond to variations in demand, voltage and frequency deviations, or other system-wide changes. The system response includes adjusting power flows, voltage regulation, frequency control, and stability maintenance. When the power system experiences a disturbance or a change in demand, the response mechanism aims to restore equilibrium and ensure a continuous and reliable electricity supply. For example, in the case of a sudden increase in demand, generators need to ramp up their power output to meet the increased load. This response involves adjusting the control settings of the generators and coordinating their actions to maintain a stable frequency and voltage within

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

acceptable limits. Similarly, when there is a fault or outage on a transmission line, the system response involves rerouting power flows and redistributing the load to ensure that all areas are adequately supplied.

As discussed in previous sections, the pre-conditions and initiating events can significantly increase the path reactance and decrease the rotor angle stability margin of the system. Figure 34 shows the BB4 regarding the system response. The increase in path reactance implies that the power system becomes less capable of accommodating changes in demand or disturbances. This higher reactance affects the speed at which power flows through the network and the stability of the voltage profiles. With higher path reactance, the system's response to load fluctuations or other disturbances may be delayed, leading to slower adjustments in voltage and frequency.

Moreover, the reduction in rotor angle stability margin further amplifies the power system's response vulnerability. This delay in response can lead to voltage and frequency deviations, compromising the system's stability. Voltage instability, resulting from delayed voltage regulation, can trigger a chain of events, including voltage collapse, load shedding, and the tripping of transmission lines or generators. These events can further disrupt the system's equilibrium and initiate cascading failures.

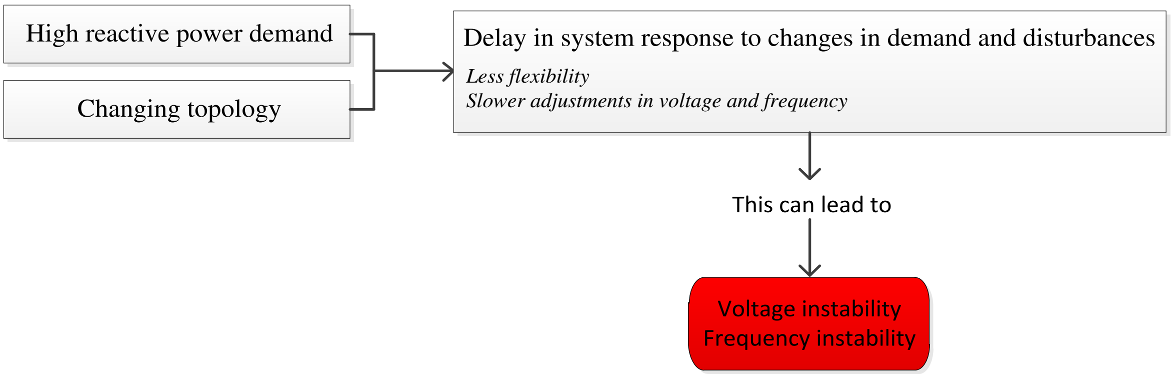

High reactive power demand
Changing topology
Delay in system response to changes in demand and disturbances
Less flexibility
Slower adjustments in voltage and frequency
This can lead to
Voltage instability
Frequency instability

Figure 34. BB4: system response

e) BB5: Frequency instability

Frequency instability is a critical aspect of power system stability that can lead to cascading failures and blackouts. From the pre-condition perspective, the main causes of frequency instability are sudden changes in load demand, inadequate reserve capacity, or the loss of generation sources for maintenance, which can create imbalances in the supply-demand equilibrium. Besides, initiating events, such as the sudden loss of a large generator or a major transmission line, can further exacerbate frequency instability. To be more specific, when a fault occurs, protective relays detect the fault and isolate the affected section by tripping circuit breakers. This sudden loss of a transmission line can result in an imbalance between generation and load. The immediate consequence of a fault-induced outage is a reduction in available transmission capacity, which can lead to increased power flows on alternate paths. These increased flows may exceed the thermal limits of the remaining transmission lines and increase active and reactive power losses, and the same issue in BB2 may occur. As a result, corrective actions such as generator tripping or load shedding may be

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

necessary to prevent further instability. This can trigger a chain of events that further exacerbates frequency instability. For instance, an outage of a transmission line due to pre-conditions or a fault can increase the reactive power demand in the network. Generators respond by attempting to supply the additional reactive power, which can result in over-excitation or loss of excitation (BB4). These generator-related issues can contribute to frequency deviations and exacerbate the system's instability.

Moreover, the operation of protection schemes can have unintended consequences on frequency stability. For instance, protection relays may trip transmission lines or generators during a fault event to isolate the faulted component and prevent further damage. These protective actions can result in an abrupt loss of generation capacity or a reduction in the available transmission paths, leading to a sudden frequency drop. Figure 35 provides the overall mechanism of frequency instability in terms of cascading failures.

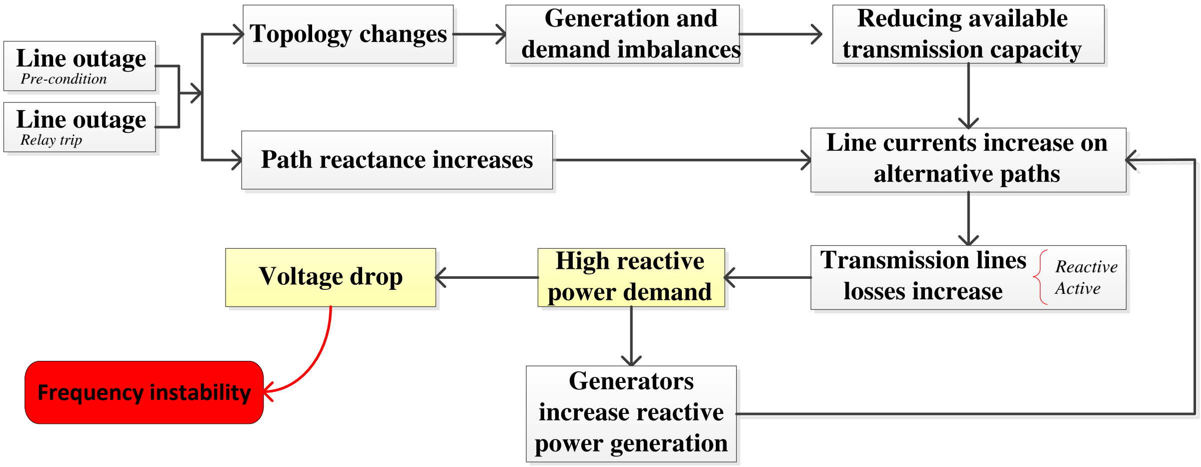

Line outage
Pre-condition
Line outage
Relay trip
Topology changes
Generation and demand imbalances
Reducing available transmission capacity
Path reactance increases
Line currents increase on alternative paths
Voltage drop
High reactive power demand
Transmission lines losses increase
Reactive
Active
Frequency instability
Generators increase reactive power generation

Figure 35. BB5: Frequency instability

3 Annex III: Simulation results for cyber-attacks on EVCS

3.1 Power system modelling

Power systems modeling is sophisticated and challenging due to several reasons. Firstly, power systems are highly dynamic and nonlinear in nature, with multiple components interacting with each other in complex ways. Secondly, power systems are subject to various disturbances, such as faults, voltage sags, and blackouts, which can affect their behavior in unpredictable ways. Thirdly, power systems are subject to many external factors, such as weather conditions, changing demand patterns, and fluctuations in the availability of RES, which can affect their behavior and make modeling challenging. Furthermore, power systems are subject to various regulations and standards, which must be taken into account in their modeling. To accurately model power systems, engineers and operators must have a deep understanding of the physics and mathematics underlying the behavior of power systems, as well as access to accurate data on system parameters and operating conditions. They must also have access to advanced modeling tools and software, which can help them to simulate the behavior of power systems and predict their performance under different scenarios.

Since implementing a thorough power system model is laborious, obtaining an appropriate test model for each application is crucial. This study aims to analyze the impact of EVCS cyber-attacks on the power system, specifically cascading failures and blackouts. Accordingly, a well-designed power system modeling is required to simulate the actual behavior of the power system during cascading failures. In the literature, several approaches are employed to model cascading failures. These approaches can be roughly classified into six categories based on their different characteristics (H. Guo et al., 2017), such as topological models, stochastic simulation models, high-level statistical models, dynamic simulation models, interdependent models, and other models.

Dynamic simulation models can simulate interactions under multi-contingency cases during cascading failure. Additionally, various mechanisms can be included in dynamic simulation to represent the system more accurately. Dobson et al. (Dobson et al., 2005) introduce a branching process to model the exponentially increasing phase of cascading blackouts. Authors (Mei et al., 2009) proposed an improved OPA model to address the significant gap between simulation and practice and the low accuracy of the probability distribution of blackout size. Reference (Nedic et al., 2006) introduces a new cascading failure blackout model using AC power flow to identify critical loading with a significant risk of large blackouts. A new dynamic model of cascading failure in power systems, Cascading Outage Simulator with Multiprocess Integration Capabilities (COSMIC), using has been introduced using quasi-steady-state (QSS) simulation (Song et al., 2016). The proposed model is able to simulate a power system with a set of hybrid discrete and continuous differential algebraic equations, protection systems, and machine dynamics. Transmission Reliability Evaluation of Large Scale Systems (TRELSS) is a commercial

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

cascading failure analysis tool that can examine the cascade propagation using a quasi-steady state simulation and protection and control model (Bhavaraju & Nour, 1992).

Since each of the previously proposed models is implemented based on the specific needs and objectives of their works, they may not be suitable for the study. Most of them just used simple DC or AC power flow approaches to simulate power system behavior or neglect the protection system role. Therefore, a test model was implemented in this model to simulate the real-world behavior of the power system in case of a cyber-attack on EVCS. In the following section, the technical details of employed power system modeling are provided.

3.1.1 Power system test bench

In order to investigate the load-altering attack impact on the power system, it is critical to understand how the power system will behave in case of changing load in the time domain simulation. More importantly, as the protection system plays an influential role in cascading failure propagation, identifying the protection relay’s mechanism is essential in this study. Hence, a comprehensive power system model has been utilized, including power system dynamics and protection schemes. This model is implemented based new England IEEE 39 bus test system using DigSILENT Power Factory 2021. The single-line diagram of the grid is shown in Figure 36. The full details of the 39 bus system are presented in Table 7.

Table 7. Characteristics IEEE 39 bus system

NO	Characteristics	Value
1	Frequency	60 Hz
2	Voltage Level	345 KV
3	Bus count	39
4	Line count	46
5	Generator count	10
6	AVR	IEEE Type 1
7	Total Active Load	6247.7 MW
8	Total Reactive load	1453 MVar

In order to cover the dynamic response of the system in the time domain simulation, the AVR and governor controllers are also included in the model.

This project has received funding from the European Union’s
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

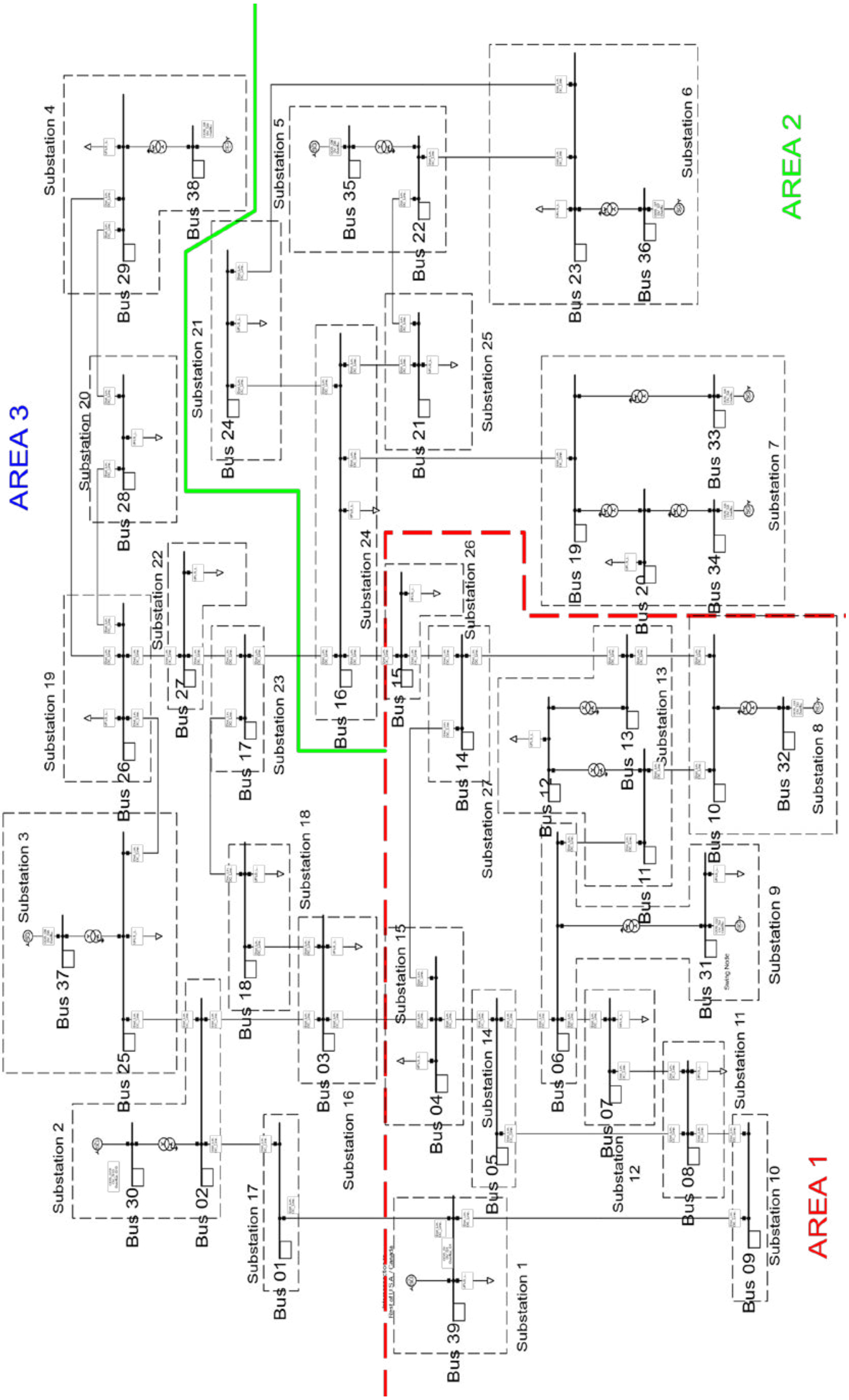


Figure 36. SLD of IEEE 39 Bus system

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

3.2 Simulation results

Since an EVCS performs as a variable load in the power system, the impact of a cyber-attack can be modeled as load-altering attack. For example, the intruder can decrease the load suddenly by cutting off all EVs in the charging station. Therefore, EVCS cyber-attack effects on cascading failures can be analyzed through different load-altering scenarios. To analyze the impact of load manipulation, the following three main case studies are investigated: decrease, increase, and combined attacks. In terms of attacker challenges (maybe: the resources required by the attacker), cutting EVCS off is the most straightforward approach to alter the total demand of the power system (maybe: the consumption in the connected bus). As a result, load decreasing has the most possibility to happen, and it is considered the main case to analyze.

In order to find the threshold which causes a cascading failure, a brute-force search is applied. In the employed method, demand, including both active and reactive power, is changed gradually to cause large disturbances and initiate cascading outages. For load manipulation, the load either decreased or increased equally based on the manipulation ratio. The manipulation ratio is a proportion that indicates how much of the load should be altered. In this study minimum manipulation ratio is 5%, and it will be increased by a step of 5% to reach the critical threshold. It is worth mentioning that the total simulation time is limited to 30s to consider the only effect of the Frequency Containment Reserve (FCR), which is the governor's response. The following section investigates various simulation scenarios to indicate how a cyber-attack on EVCS can initiate a cascading failure and lead to a blackout.

3.2.1 Case A: load decrease

In this case, the total load of the power system will be decreased by manipulation ratio, and then the effect of this event will be investigated throughout the system. Table 8 summarizes essential details of load decreasing attack form ratio 5% up to 35%. As can be observed, with increasing the manipulation ratio, the impact of load-altering would be more severe, affecting both the frequency and voltage of the power system. Moreover, load decreasing may trigger some protection relays due to sudden changes in power. For example, a distance relay was operated when the load was decreased by 15%. In this scenario, not only was distance protection operated, but also the over-frequency relay of generators reacted and tripped some generators.

Table 8. Overview of load decreasing impact on power system for manipulation ratios

Manipulation ratio (%)	Min Frequency (Hz)	Max Frequency (Hz)	Min Voltage (p.u.)	Max Voltage (p.u.)	Protection events	Time of event
5	60	60,4323	0.982	1.07	**-**	-
10	60	61,0056	0.982	1.084	-	-
15	60	61,5863	0.951	1.1007	Dist. Line 1-39	2,061667s
20	60	62,1423	0.9225	1,1186	Dist. Line 1-39	2,011667s
25	60	62,7094	0,8193	1,1383	Dist. Line 1-39	2,0083s

Manipulation ratio (%)	Min Frequency (Hz)	Max Frequency (Hz)	Min Voltage (p.u.)	Max Voltage (p.u.)	Protection events	Time of event
30	60	63,3743	0,6962	1,1633	Dist. Line 1-39	2,016342
35	60	63,93165	0,1512	1,2036		

Although the power system witnessed a major mismatch between demand and generation in this scenario, the generators' governor succeeded in maintaining the frequency, and it didn't lead to widespread cascading failures. As it is shown in Figure 37 and Figure 38 system is stable in terms of voltage and rotor angle in this scenario.

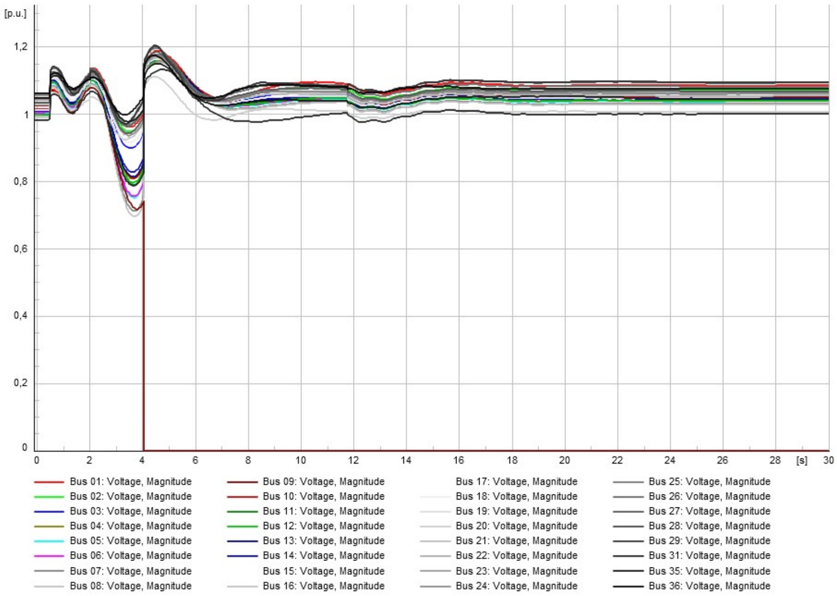


Figure 37. Voltage magnitudes of buses for simulation Case A1: Load reduction by 35%

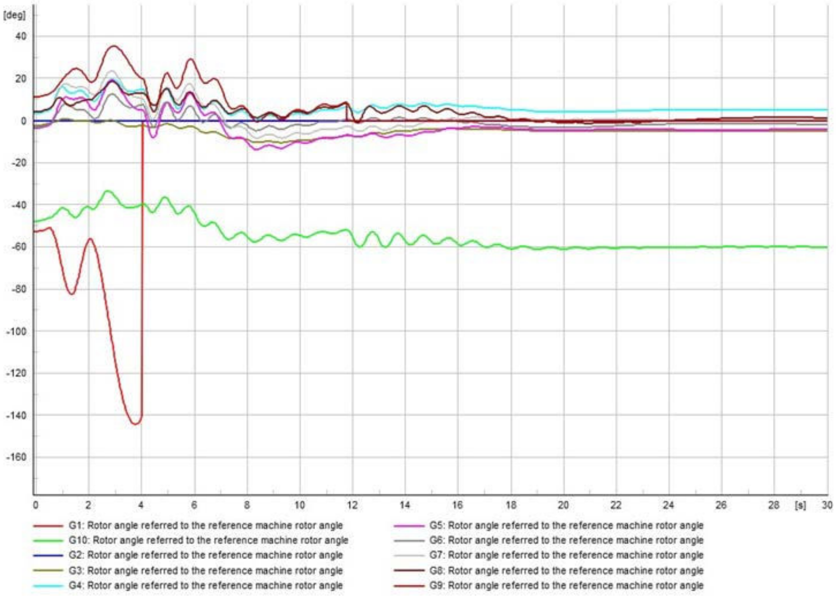


Figure 38. Rotor angle of generators for simulation Case A1: Load reduction by 35%

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

In the second scenario, the manipulation ratio increased by 1%, resulting in a total load decrease of 36%. This attack caused widespread cascading failure and led to a blackout.

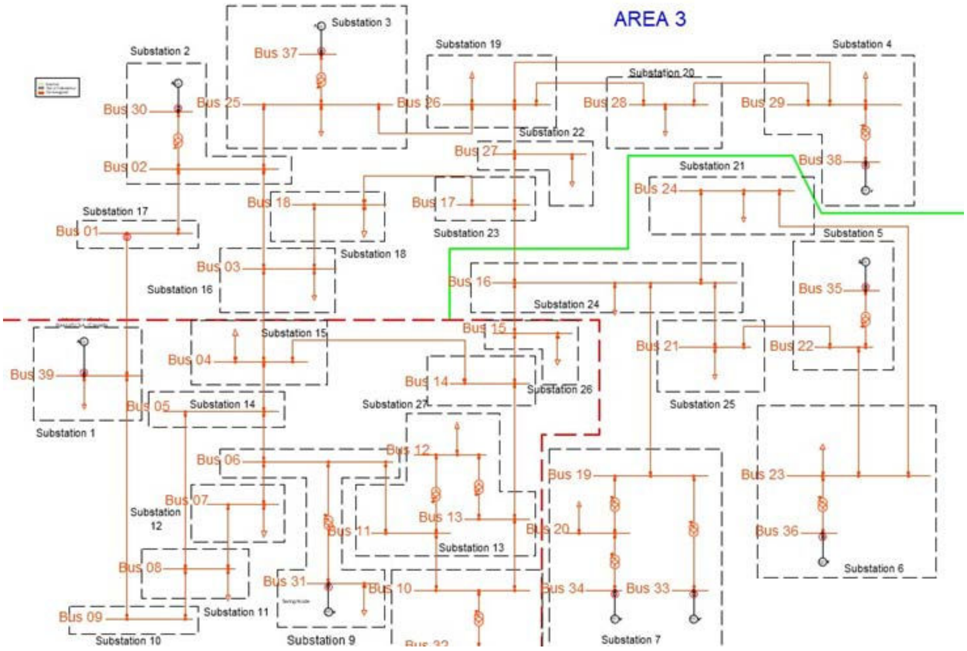
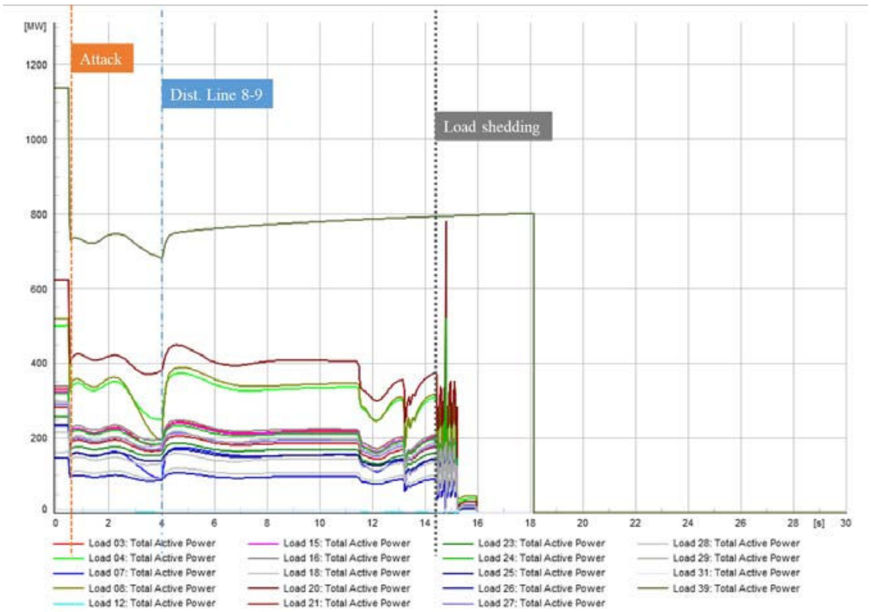


Figure 39. SLD of IEEE 39 bus - Case A2: Load reduction by 36%

With load reduction, frequency starts rising, which leads to over-frequency issues in the power system. Eventually, over-frequency protection tripped some of the generators and reduced the overall generation capacity of the power system. As a result, the over-frequency issue becomes the under-frequency problem because of the lack of generation, as seen in Figure 41. From Figure *40*, it can be overserved that after 14s, the UFLS relays start to operate and reduce the load. However, the system cannot maintain the frequency and widespread cascading occurred in the power system. In such circumstances, the system is also faced with large voltage disruptions and then collapses, as can be seen in Figure 42.



This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Figure 40. *Active power of all loads for simulation Case A2: Load reduction by 36%*

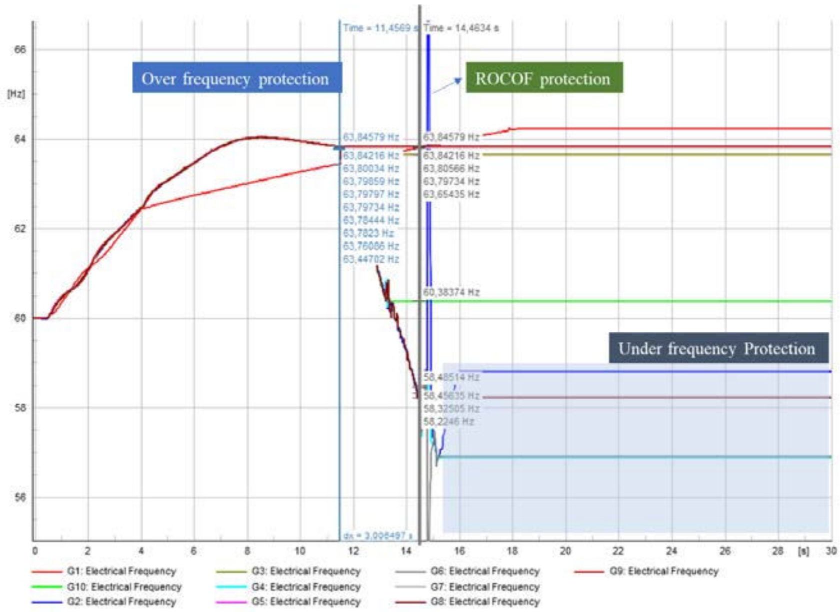


Figure 41. Electrical frequencies for simulation Case A2: Load reduction by 36%

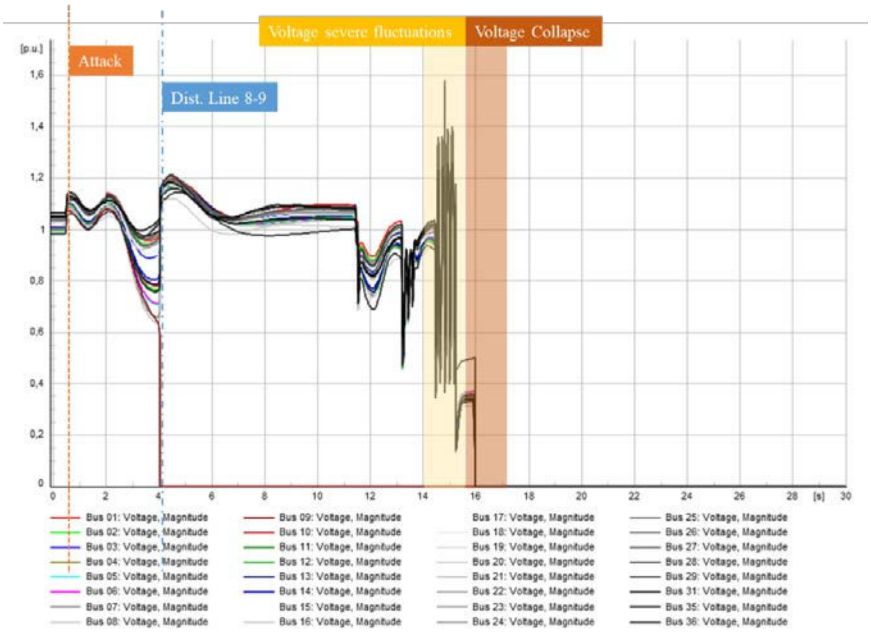


Figure 42. Voltage magnitudes of buses for simulation Case A2 Load reduction by 36%

3.2.2 Case B: load increase

In this section, the load-increasing attack and how it can initiate a cascading failure will be analyzed. In the first scenario of this case, the demand was increased in all loads by 35%, so the power system faced a demand manipulation attack. In this scenario, the generators' governor tried to maintain the frequency; however, they couldn't prevent the frequency drop because of the substantial change in the loads. Subsequently, the UFLS relays were operated to balance the generation with demand by shedding extra load.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

The load-shedding events can be easily noticed in Figure 44. Moreover, as seen in Figure 43, the frequency recovered after decreasing the demand.

It should be noted that even with load shedding, a cascading failure occurred in the power system, as illustrated in Figure 45. Because of the frequency drop, generator G9 is tripped by an under-frequency relay, causing a cascading failure in the nearby area. However, this cascading event did not lead to a complete blackout and caused an islanded outage. The voltage magnitude and rotor angle plot are presented in Figure 46 and Figure 47, respectively.

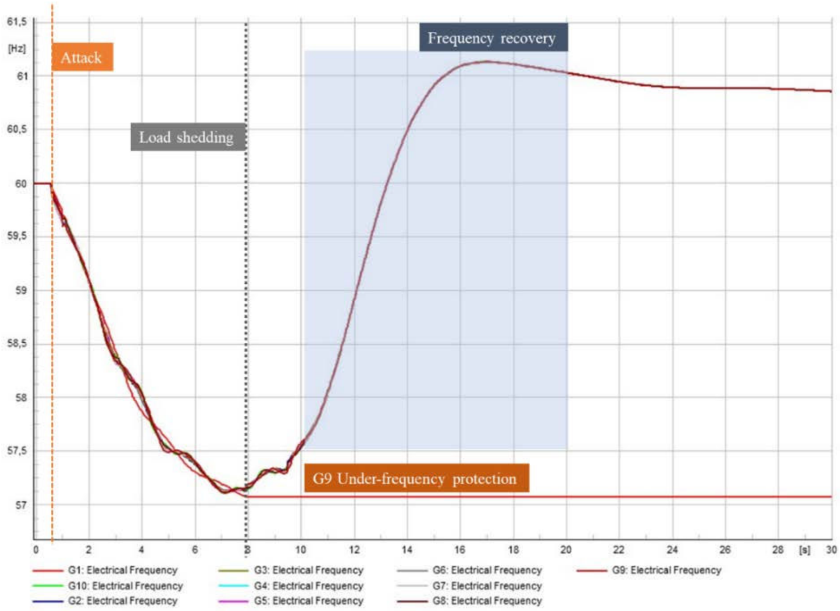


Figure 43. Electrical frequencies for simulation Case B1: Load increase by 35%

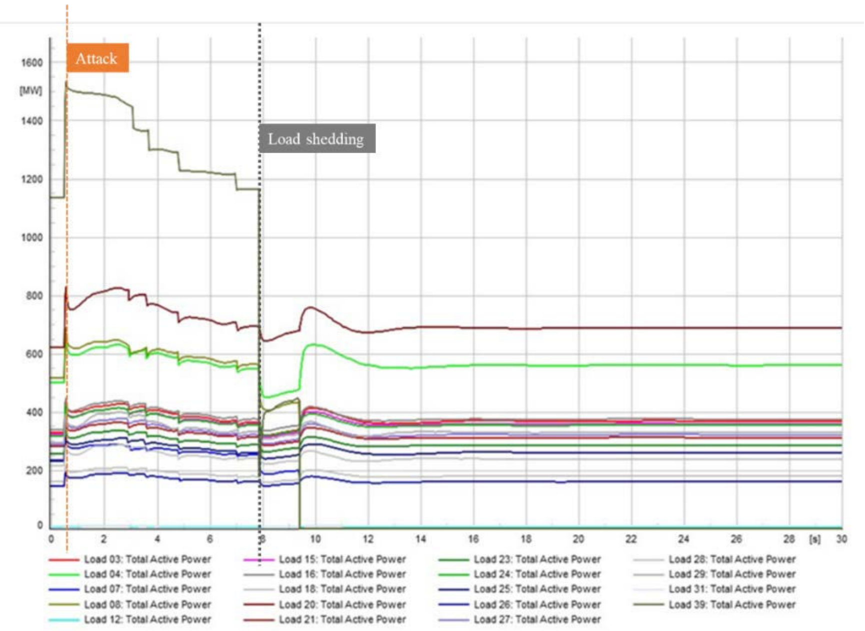


Figure 44. Active power of all loads for simulation Case B1: Load increase by 35%

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

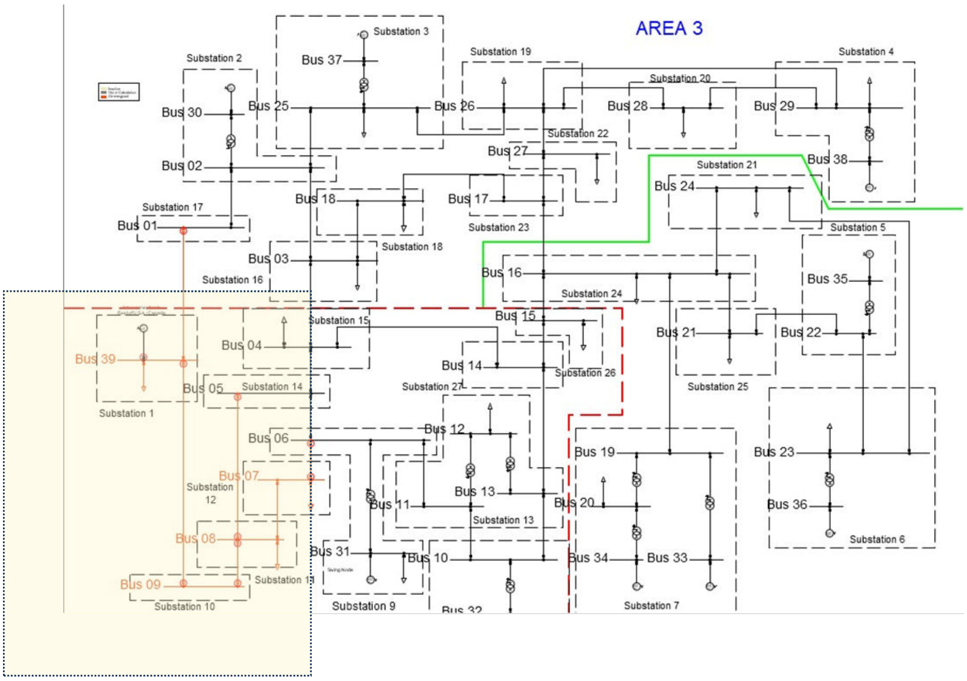


Figure 45. SLD of IEEE 39 bus - Case B1: Load increase by 35%

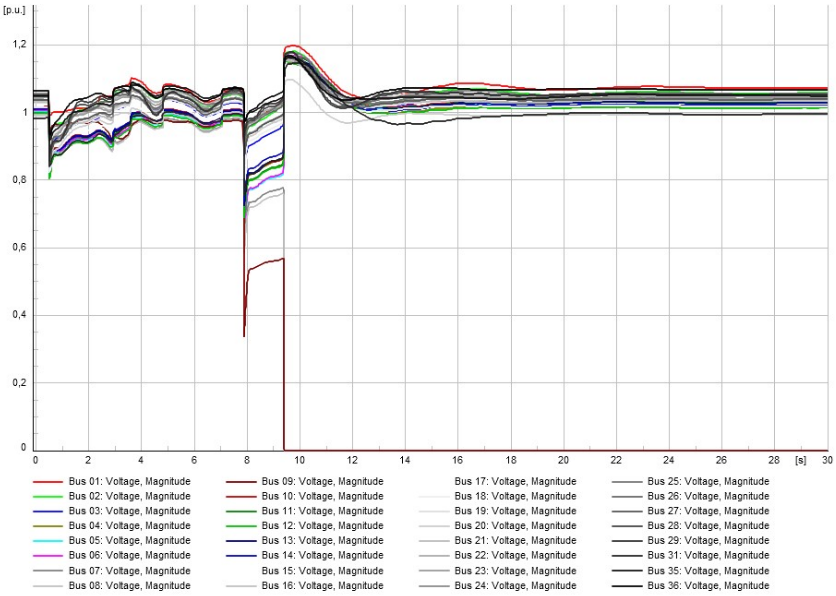


Figure 46. Voltage magnitudes of buses for simulation Case B1: Load increase by 35%

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

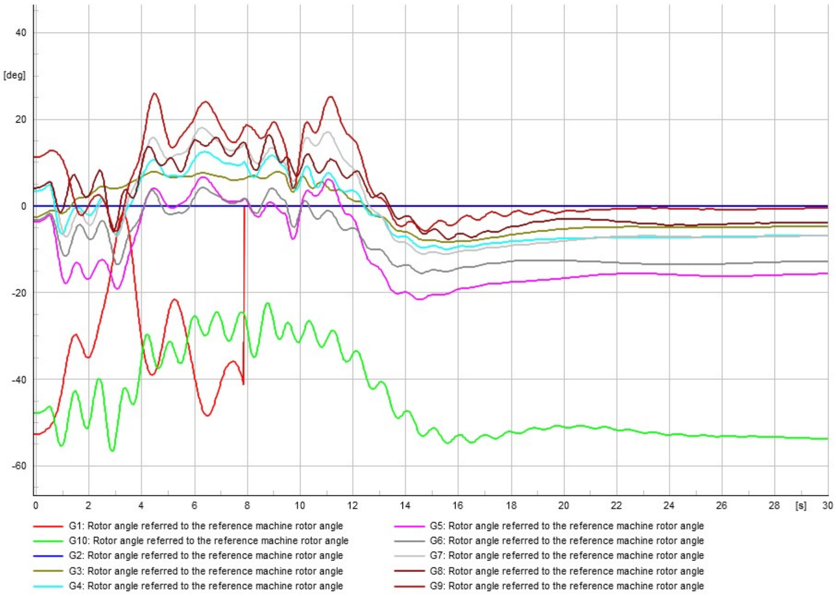


Figure 47. Rotor angle of generators for simulation Case B1: Load increase by 35%

In the second scenario, the magnitude of load manipulation increased by 1%, resulting in a total load increase of 36%. This attack can cause a widespread cascading failure and lead to a blackout. The load shedding conducted by UFLS relays is insufficient to prevent the blackout. As seen in Figure 48, the system lost synchronism around 7s, leading to system instability and the operation of relays to trip lines and generators.

In comparison with load reduction, increasing load may cause cascading failure in a shorter period. Since overload reduces the frequency instantaneously, it triggers the UFLS relays faster. Voltage magnitude and rotor angle plots are presented in Figure 49 and Figure 50, respectively.

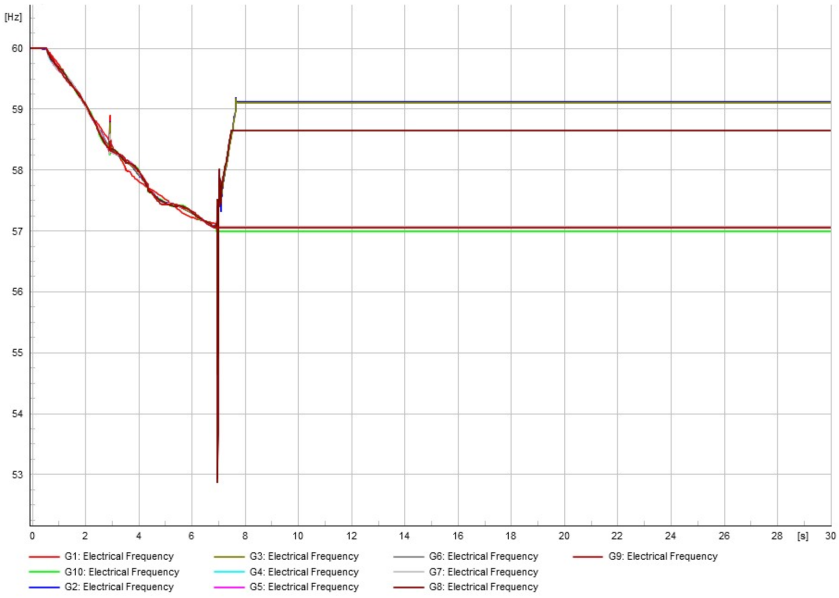


Figure 48. Electrical frequencies for simulation Case B2: Load increase by 36%

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

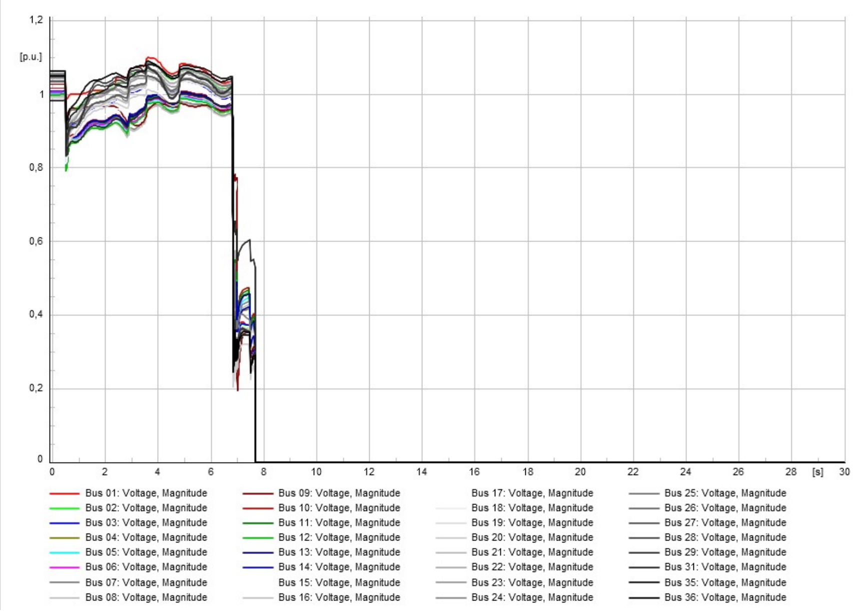


Figure 49. Voltage magnitudes of buses for simulation Case B2: Load increase by 36%

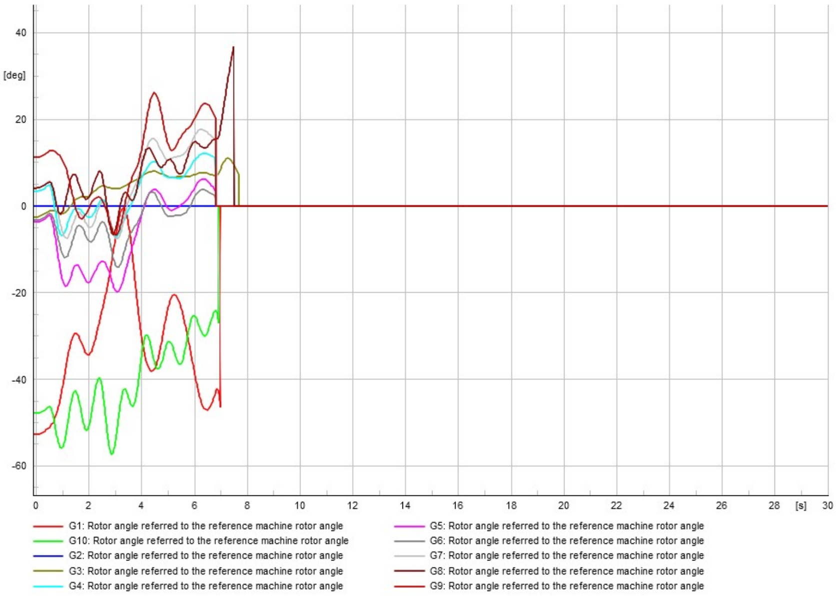


Figure 50. Rotor angle of generators for simulation Case B2: Load increase by 36%

3.2.3 Case C: combined attack

In this case, two combined scenarios were implemented to show the impact of sequential decreasing and increasing loads on cascading failures in power systems. So in the first scenario, all available loads were decreased by 36% at 0.5s, then in 1s, all loads increased by 36% and went back to normal state. Evidently, this demand manipulation can not cause any significant disturbance in the power system, as demonstrated in Figure 51. Electrical frequencies for simulation Case C1, frequency of generators did not see any critical issue.

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

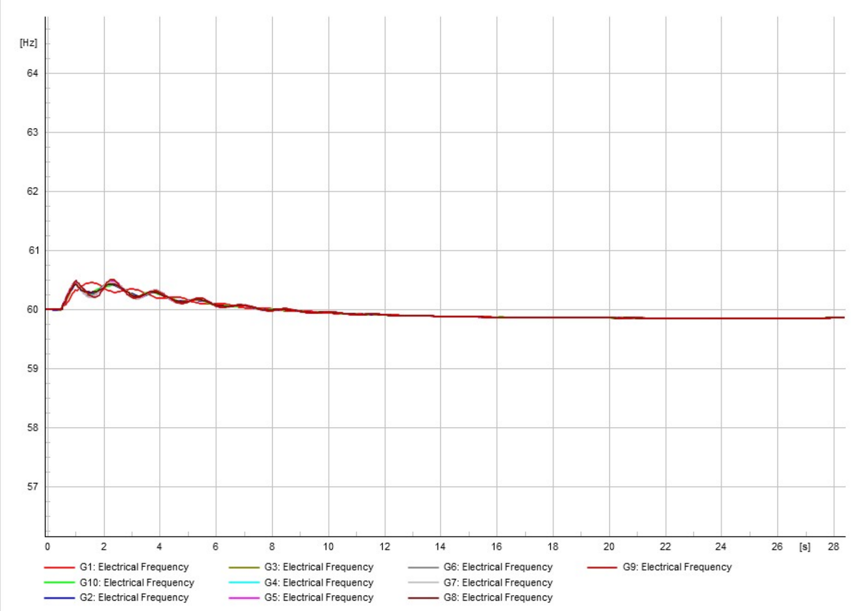


Figure 51. Electrical frequencies for simulation Case C1

In the second scenario, the same pattern was used but with more delay between load changes resulting in a total load decrease of 36%. This attack can cause a widespread cascading failure and lead to a blackout.

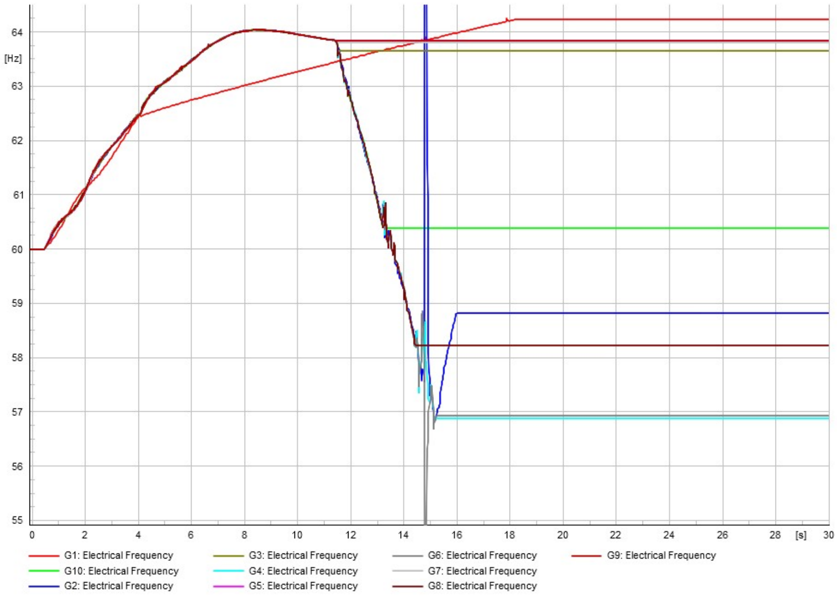


Figure 52. Active power of all loads for simulation Case C2

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

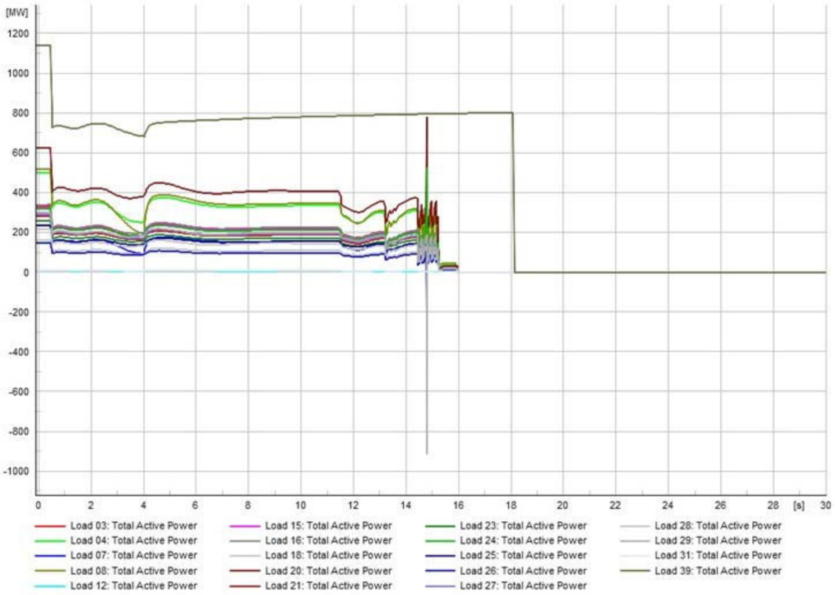


Figure 53. Electrical frequencies for simulation Case C2

3.3 Conclusion

This section investigates the potential effects of load-altering attacks on power systems through cyber-attacks on EVCS. The primary goal of this study was to understand how load attacks can lead to cascading failures and ultimately result in a blackout. To achieve this objective, realistic protection schemes and dynamic models were fully implemented in the IEEE 39 bus system using Power Factory DIgSILENT. Three different demand manipulation scenarios were also considered to obtain a comprehensive understanding of load-altering attacks and cascading failures. The first step in this study was to gradually increase the rate of manipulation algorithms to investigate the effect of load change percentage on power system dynamic response. The results showed that there is a critical manipulation ratio of load increasing or decreasing that can cause a cascading failure and lead to a blackout. These findings highlight the potential dangers associated with load-altering attacks and the need for robust protection schemes.

Moreover, the study also examined the pivotal role of the protection system and its contribution to cascading failure propagation. While protection relays are designed to maintain the stability of power systems, they can also play an influential role in cascading failures. The results showed that the protection system's sensitivity settings significantly affect the cascading failure propagation, and improper protection settings can exacerbate the impact of load-altering attacks. Overall, this study provides valuable insights into the potential impacts of load-altering attacks on power systems and emphasizes the need for robust protection schemes to prevent cascading failures and blackouts. It is important to note that the study's findings are based on simulations using a specific power system model, and further research is needed to validate the results and generalize them to other power systems.

4 Annex IV: Modelling details for MaDIoT attacks

The models, assumptions, and scenarios considered in the study carried out within T2.2 are described below.

4.1 Models

To compare the impact of MaDIoT attacks on two different systems, the following power system models were used in the study carried out within T2.2:

- **IEEE 39-Bus System**: Known as the New England power system, it consists of 39 buses, with a total base load of 6097.1 MW of active power and 1408.9 MW of reactive power. Since it is an American system, the electrical frequency is 60Hz. This test system uses a dynamic load model.
- **PST-16 (simplified European model):** Known as the PST-16 Benchmark System (Rueda et al., 2014), it consists of three areas (A, B, C) and 66 buses, with a total base load of 15565 MW of active power and 2225 MVar of reactive power. The electrical frequency is 50Hz (European system).

  This system model uses the constant impedance load model (Rueda et al., 2014) for details on how the bulk generators are modeled, as well as to view the complete grid diagram, refer to (Rueda et al., 2014).

  Figure 54 shows a simplified representation of the PST-16 system. Area A may be representative of the north of Europe, with a high share of hydroelectric generation, whereas areas B and C could represent central and south Europe, respectively, with high shares of thermal and nuclear. Area C concentrates the loads (demand > generation capacity), so areas A and B must support C through two connections.

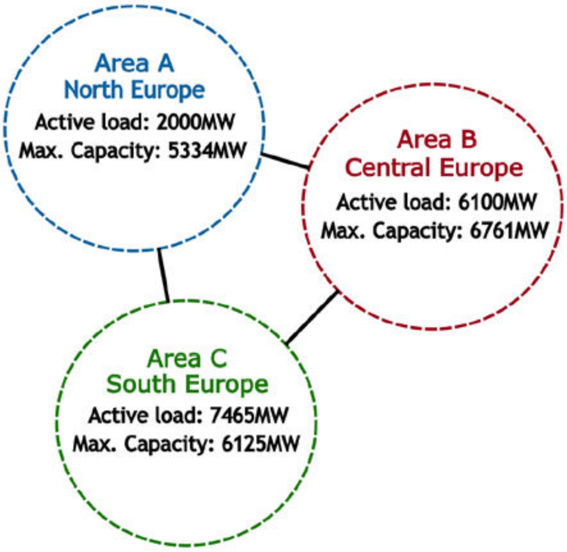


Figure 54. Simplified representation of the PST-16 benchmark model.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Regarding the protections added to the system models for analysis, four were considered:

1. Overvoltage protection (actuating when voltage > 1.1 p.u for 10s)
2. Undervoltage protection (actuating when voltage < 0.85 p.u for 10s)
3. UFLS protection (following the scheme presented in Table 9)
4. OFGR protection (actuating when the frequency is 51.7 Hz in the PST-16 or 61.7 Hz in IEEE 39, similar values to those used by (Huang et al., 2019b))

Table 9. UFLS scheme applied for the PST-16 (50Hz) and IEEE 39 (60Hz) models.

Frequency threshold (Hz)	59 49	58.8 48.8	58.6 48.6	58.4 48.4	58.2 48.2	58 48
Load shed (%)	5	5	10	10	10	10

4.2 Assumptions and scenarios

In the study carried out within T2.2, every compromised load (i.e., bot) is assumed to consume 3 kW of active power (Shekari et al., 2022). To keep the power factors like those in the baseline test systems, the attack would also affect the reactive power. The power factor of the demand (inductive) for the IEEE 39-bus and PST-16 systems are 0.97 and 0.99, respectively. Therefore, the reactive power of the bot is 0.69 KVar for the IEEE 39-bus system and 0.42 kVar for the PST-16 system. Only MaDIoT attacks that increase power consumption are considered (Shekari et al., 2022).

The attacks would only affect three nodes that are selected randomly, in a Monte Carlo-like way, for each simulation, as opposed to the approach in (Shekari et al., 2022), where the most-vulnerable nodes were compromised in the attack. Therefore, it is assumed that the attacker does not have detailed knowledge about the power system.

For the simulations in the PST-16 system, the loads attacked belong to the same area, as the closer they are, the higher the expected impact on the system (Shekari et al., 2022). The attacks are performed at t=1s and are considered successful if, by the end of the simulation, loads have been shed (tripping of UFLS, overvoltage, or under-voltage protections) or if generators had to be disconnected (OFGR protections). This criterion is similar to the one in (Amini et al., 2018).

Table 10 shows the scenarios executed for each system. For each scenario, the botnet size varies in the range [50k, 500k], in 50k steps, and 21s are simulated to reduce the computational load. For the PST-16 system, nearly 1500 simulations were performed, while the IEEE 39-Bus accounts for 424 simulations.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

Table 10. Scenarios for analysis of MaDIoT attacks.

Scenario	Test system	Area	Botnet size	# Nodes attacked
US39	IEEE-39	-	[50k, 500k]	3
EU-A EU-B EU-C	PST-16	A B C		

This project has received funding from the European Union's Horizon Europe Energy Research and Innovation programme under Grant Agreement No 101075665.

5 Annex V: Resilience actions

5.1 Frequency control on low–inertia power grids

5.1.1 State of the art

Measures to ensure the frequency stability of the UCTE are mandatory, e.g., by the commission regulation (Union, 2016). The regulation establishes a network code that lays down the requirements for grid connection of power-generating facilities, namely synchronous power-generating modules, power park modules, and offshore power park modules, to the interconnected system. In particular, type C and D power-generating modules shall be capable of providing FCR.

Within a synchronous area, the FCR is dimensioned to keep the system frequency within a defined operational range based on a reference incident. For example, the relevant design criteria for the continental Europe synchronous area are to keep the system frequency within 50.0 Hz 200 mHz in case of a load imbalance of 3.000 MW.

The Final Report on the System Disturbance on 4 November 2006, which was published by the union for the co-ordination of transmission of electricity (UCTE, 2006), shows the extent of the threat that needs to be controlled. The report reveals an instantiations power imbalance of more than 10.000 MW for the split-caused North-Eastern synchronous area, i.e., approximately 17% of total generation in this area before the splitting.

Against this background, future measures to enhance frequency stability are launched with the European Network of Transmission System Operators for Electricity's (ENTSOE) implementation guidance documents, e.g., with:

- "Limited frequency sensitive mode" (Broderick, 2018a) helps to determine the main criteria/motivation for the specifications of the limited frequency sensitive mode capabilities of power generating modules at the national level.
- "Frequency Ranges" (Ndreko, 2021) provides a detailed explanation of frequency ranges required capability for facilities connected according to NC RFG, NC High-Voltage DC (HVDC), and NC DC and proposals on its implementation for each synchronous area.
- "Need for Synthetic Inertia (SI) for frequency regulation" (Broderick, 2018b) provides guidance on SI aspects to be considered when choosing relevant national parameters and opting in or out of nonmandatory requirements.
- "ROCOF withstands capability" (Broderick, 2018c), aiming at ensuring that power-generating modules, demand units offering Demand Response (DR) services, HVDC systems, and DC-connected power park modules shall not disconnect from the network up to a maximum rate of change of frequency.
- "Parameters related to frequency stability" (Broderick, 2016) provides parameters related to frequency stability issues. It aims to give orientation to define the related non-exhaustive technical requirements.

5.2 Interarea oscillation vulnerability and resilience actions

Recent studies show that interarea oscillations have been responsible for several large-scale power system failures in different parts of the world, such as the following examples.

- The 1996 Western System Coordinated Council (WSCC) blackout: this blackout, which affected the western United States and parts of Canada, was caused by an interarea oscillation that originated in Oregon and quickly spread throughout the interconnected system. The oscillation caused generators to trip offline, resulting in a cascading failure that ultimately led to the blackout (Kosterev et al., 1999).
- The 2003 Northeast Blackout in North America: this blackout, which affected parts of the northeastern United States and Canada, was caused by an interarea oscillation that originated in Ohio and quickly spread throughout the interconnected system. The oscillation caused transmission lines to overload and trip offline, which led to a cascading failure and the subsequent blackout (Chadwick, 2013).
- The 2018 South American blackout: this blackout, which affected Argentina, Uruguay, and parts of Brazil, was caused by an interarea oscillation that originated in a power plant in Argentina. The oscillation caused the failure of the transmission network and led to the loss of power for millions of people.
- The 2016 European failure: this power system failure is more recent, and a closer example is the unexpected opening of a line in the French system (on the western 400 kV interconnection corridor with the Spanish system) that triggered an oscillatory incident in the Continental Europe electricity system in December 2016 (ENTSO-E SG SPD REPORT, 2017).

To solve the problem of interarea oscillation, the detection and damping of oscillations between interconnected generators constitute a significant concern to anticipate and mitigate (Klein et al., 1991). For damping the oscillation, controls such as Power System Stabilizer (PSS) for generators and power oscillation damping in Flexible AC Transmission System (FACTS) are utilized in the power system. However, the detection functions of interarea oscillation are still under development, being the most studied Fast Fourier Transform (FFT), Prony Analysis, and Matrix Pencil Method (MPM). These functions can anticipate the spread of the interarea oscillation, being a resilience action to prevent the damage that can cause the spread of an interarea oscillation throughout the electric grid.

- The FFT can be used to analyse the frequency content of power system signals and identify the presence of power oscillations and their frequencies and determine the oscillation modes (Panda et al., 2016; W. Xiong et al., 2020).
- The Prony analysis is a least square approximation technique of fitting a sum of exponential terms to the measured data. It identifies the amplitudes, damping factors, frequencies, and phase angles inside the data. Different authors use the Prony analysis to monitor interarea oscillation (Foyen et al., 2018; Ning Zhou et al., 2010).
- The MPM approximates a given signal by a sum of complex exponentials. The idea originates from the approach of pencil-of-function. This method uses Hankel matrices and Singular Value decomposition to fit complex

exponential sums. MPM finds all parameters, i.e., the magnitude, the damping factor, the frequency, and the phase angle. The MPM is also used for oscillation monitoring.

The table reported below provides a comparison between the different parameters that can be obtained using the three methods studied in this article where:

- f: frequency
- α: damping
- A: amplitude
- Θ: phase angle
- Wave: original wave reconstruction

Table 11. Comparative between the parameters

Method	f	α	A	θ	Wave
FFT	Yes	No	Yes	No	No
Prony Analysis	Yes	Yes	Yes	Yes	Yes
MPM	Yes	Yes	Yes	Yes	Yes

Performing a theoretical comparison, the FFT method is computationally efficient and easy to implement, making it a popular choice in signal analysis (W. Xiong et al., 2020). However, it has some limitations. The accuracy of the results depends on the number of samples taken, and noise in the measurements can affect the results. In addition, the FFT is affected by the phenomenon of spectral leakage and the picket effect(J. Li et al., 2018). As the FFT converts a time-domain measured signal into its frequency-domain representation, only the peaks of the frequency of the measured signal are obtained. Thus, the damping is not calculated.

Prony analysis has some advantages, such as being able to handle non-stationary and non-linear signals and providing accurate results with a small number of samples (Wilson et al., 2019). Moreover, Prony analysis retrieves the damping information, which is not possible from the conventional FFT. The original signal can be reproduced since the amplitude and phase angle are also calculated. However, it can be sensitive to noise in the measurements and may require careful selection of model order. Moreover, Prony analysis requires high computational time(Chitturi et al., 2014).

The matrix pencil method agrees with some Prony advantages, such as being able to handle non-stationary and non-linear signals. However, MPM requires less computational time compared to Prony analysis and improves its performance concerning accuracy, efficiency, and noise sensitivity (Chitturi et al., 2014). As with the Prony analysis, MPM retrieves the damping information, which is not possible from the conventional FFT. The original signal can be reproduced since the amplitude and phase angle are calculated.

In general conclusion, all three functions can detect interarea oscillation, which is a resilience action to prevent the propagation of inter-area oscillation throughout the power grid. The FFT could be used when computational time takes priority over the accuracy of the results. When run time is not so important and accurate damping and frequency results are required, Prony analysis and MPM are a better choice, with MPM being more accurate.

This project has received funding from the European Union's
Horizon Europe Energy Research and Innovation
programme under Grant Agreement No 101075665.

5.3 Resiliency actions at the cyber layer

cybersecurity-related actions enumerated in the ISO/IEC 27002:2022, the IEC 62443-2-1, the NIST 800-32r3, and the 11 Strategies for a successful SOC and grouped these actions under the NIST cyber resiliency goals are extracted. Through the exercise, it can be observed that cybersecurity actions mentioned in the state-of-art refer to a common set of categories. These categories are listed in bold in the second column. The actions listed under each category do not intend to cover the content of the state-of-art documentation in full. Rather, the selected actions intend to be a representative set of the actions and related cybersecurity topics that the documents discuss.

Table 12. Aggregation of actions with respect to NIST Cyber Resilience

Aggregation of actions with respect to NIST Cyber Resilience Engineering goals	
Anticipate (identify, protect, detect)	**Assets inventory and BOM** • ISO/IEC 27002 – 5.9: Inventory of information and other associated assets • IEC 62443-2-1 – SPE 2 CM1: – Inventory management of IACS hardware/software components and network communications • NIST 800-82r3 - ID.AM: Asset management • 11 SOC Strategies – Strategy 1: Know what you are protecting and why **Governance** • NIST 800-82r3 ID.GV-2: Coordination of cybersecurity roles and responsibilities • 11 SOC Strategies Strategy 2 Mandate to operate: A SOC Charter should include direct communication, cooperation, and support with and from OT staff • 11 SOC Strategies Strategy 3 Effective SOC configuration for the Organization goals: integrated IT/OT SOC • 11 SOC Strategies Strategy 3: The SOC should participate in decisional processes concerning any aspect influencing SOC abilities • 11 SOC Strategies Strategy 3: Points of Contact people between SOC and OT environments should be assigned to remote EPES deployments **Monitor and identify threats** • ISO/IEC 27002 5.7 Threat intelligence • NIST 800-82r3 ID.RA – Risk assessment • 11 SOC Strategies Strategy 6: Tailor the collection and use of cyber threat intelligence by analyzing the intersection of adversary information, organization relevancy, and technical environment to prioritize defenses, monitoring, and other actions **Monitor environment status** • ISO/IEC 27002 8.15 Logging • ISO/IEC 27002 8.16 Monitoring activities • IEC 62443-2-1 EVENT 1.1: Event detection • IEC 62443-2-1 PR.AC – Identity Management and Access Control • NIST 800-82r3 - PR.PT-1: Logging • NIST 800-82r3 DE.AE-1: The baseline of network operations and expected data flows is established and managed • NIST 800-82r3 DE.CM – Continuous Security Monitoring • 11 SOC Strategies – Strategy 7 – Select and collect the right data from the infrastructure **Planning** • ISO/IEC 27002 5.24 Information security incident management Planning and preparation • ISO/IEC 27002 5.30 ICT readiness for business continuity • NIST 800-82r3 ID.SC – Supply Chain Risk Management • NIST 800-82r3 PR.AT – Awareness and Training

Aggregation of actions with respect to NIST Cyber Resilience Engineering goals	
	• NIST 800-82r3 RS.RP – Response Planning • NIST 800-82r3 RC.RP – Recovery Planning **Protective** measures • IEC 62443-2-1 SPE8 AVAIL2 – Backup/restore/archive • NIST 800-82r3 PR.AC – Identity Management and Access Control • NIST 800-82r3 PR.AT – Awareness and Training • NIST 800-82r3 PR.DS – Data Security [Encryption, data lifecycle management, integrity checks] • NIST 800-82r3 PR.PT – Protective Technology • NIST 800-82r3 PR.IP – Information Protection Processes and Procedures
Withstand (detect, respond)	**Monitoring and detection** • NIST 800-82r3 DE.CM – Continuous Security Monitoring • ISO/IEC 27002 5.28 Collection of evidence • IEC 62443-2-1 SPE7 EVENT1 – Event and incident management **Response** • ISO/IEC 27002 5.26 Response to information security incidents • 11 SOC Strategies Strategy 5 – Prioritize incident response: coordination between IT and OT teams • NIST 800-82r3 RS.CO – Response Communication • NIST 800-82r3 RS.AN – Response Analysis • ISO/IEC 27002 5.5 Contact with authorities • ISO/IEC 27002 5.6 Contact with special interest groups • ISO/IEC 27002 6.8 Information security event reporting • IEC 62443-2-1 EVENT 1.2: Event reporting • NIST 800-82r3 RS.CO – Response Communication **Maintain operations** • ISO/IEC 27002 5.29 Information security during disruption • ISO/IEC 27002 5.30 ICT readiness for business continuity • IEC 62443-2-1 SPE8 AVAIL1 – System availability and intended functionality (AVAIL1.1, AVAIL1.2, AVAIL1.3) • NIST 800-82r3 ID.BE-5: Resilience requirements to support the delivery of critical services for all operational states
Recover (recover)	• IEC 62443-2-1 COMP 3.4: Security patching retention of security • NIST 800-82r3 RC.CO – Recovery Communications • 11 SOC Strategies, Strategy 5 Prioritize Incident Response - Incident response in OT must be specific to the affected devices and their purpose, with varying implications of safety, availability of service, and availability of response options
Adapt (protect, recover)	**Identify improvements** • NIST 800-82r3 RS.IM – Response Improvements • NIST 800-82r3 RC.IM – Recovery Improvements • ISO/IEC 27002 5.27 Learning from information security incidents **Information Sharing** • 11 SOC Strategies Strategy 9 – Communicate clearly, share generously