Spectrum of Engineering Sciences
ISSN (e) 3007-3138 (p) 3007-312X Volume 4, Issue 3, 2026

RISK-BASED PROTECTION OF CRITICAL INFRASTRUCTURE USING INTELLIGENT DECISION SUPPORT SYSTEMS

[*1]Nasser Mohammed Alhajeri, [2]Saud Zaman Khan, [3]Fatiha Batool Rizvi, [4]Ayesha Zain

*[*1]Master Scholar, Master of Strategic Leadership, Abu Dhabi University*
[2]Graduate Scholar, Computer Science, Iqra University Islamabad
[3]Graduate Scholar, Civil Engineering Technology, Banazir Bhutto Shahed University of Technology And Skill Development Khairpur Mir's Sindh Pakistan
[4]Graduate Scholar, Computer Science, Qurtuba University of Peshawar
*[*1]roeroe1077@gmail.com, [2]saudzaman96@gmail.com [3]syedafatihashah@gmail.com [4]Khanishi007@gmail.com*

DOI: https://doi.org/10.5281/zenodo.21442457

Keywords:
Critical Infrastructure Protection; Risk Assessment; Intelligent Decision Support System (IDSS); Artificial Intelligence (AI); Digital Twin; Infrastructure Resilience; Multi-Hazard Risk Management.

Article History
Received on: 14 Feb, 2026
Accepted on: 29 March, 2026
Published on 30 March, 2026

Copyright @Author
Corresponding Author:
Nasser Mohammed Alhajeri

Abstract

Critical infrastructure is a key component to providing essential services that keeps people supplied during disasters, including energy, transportation, healthcare, water supply, telecommunications and emergency management. As physical infrastructure has become more interdependent with digital technologies, operation has become more efficient and infrastructure systems are vulnerable to a variety of physical, cyber, environmental and operational threats. Protection models such as periodical inspections and reactive response strategies are no longer effective to deal with the complexity of modern infrastructure environments. The proposed Risk Based Protection Framework Using Intelligent Decision Support Systems (IDSS) is aimed at improving the resilience and security of critical infrastructure. The proposed scope includes the integration of structured risk assessment, Artificial Intelligence (AI), Machine Learning (ML), predictive analytics, Digital Twin technology and intelligent decision support into a single architecture for proactive infrastructure management. These are broken down into seven broad stages: data acquisition, threat identification, vulnerability assessment, risk analysis, AI-based prediction, intelligent decision support, continuous monitoring. To illustrate the practical application of the proposed framework, a conceptual case study on an infrastructure for a hospital is presented. The findings show that the combination of AI and risk-based decision support can have a profound positive impact on threat detection, infrastructure monitoring, resource prioritization, emergency response planning and increase the overall infrastructure resilience. The proposed framework is flexible, applicable to different sectors of critical infrastructure, such as energy, transportation, healthcare, water management, telecommunications, airports, smart cities. The research is a step towards designing proactive and intelligent infrastructure protection strategies, which can tackle the challenges facing today's critical infrastructure systems using evidence.

1 Introduction

1.1 Background

Critical infrastructure (CI) is defined as the systems and assets that are vital to the United States' operations. These infrastructures are essential to ensure national security, economic stability and public safety. Therefore, their continuous and reliable operation is regarded as a strategic priority for governments and organizations around the world.

1.2 Problem Statement

Critical infrastructure has increasingly seen threats to it in recent years that come in a variety of shapes and forms. Natural disasters, including earthquakes, floods, hurricanes and wildfires; cyber-attacks, terrorism, sabotage, insider threats, equipment failures, and human error. As the physical world becomes increasingly connected to digital technologies, one attack can lead to failures in other industries, causing major economic and social losses.

The traditional methods of infrastructure protection are mostly based on periodic inspections, manual risk assessment and expert judgment. These approaches have been common practice, but are not always resilient to fast-changing operational scenarios and evolving threats. As a result, there is a need for more intelligent and dynamic protection strategies to enable timely and evidence-based decision making.

1.3 Importance of Risk-Based Protection:

The Risk Based Protection (RBP) approach has become a successful approach to enhancing the resilience of critical infrastructure. RBP is not the equal distribution of resources, but rather focuses protection based on the probability of an occurrence and the harm that can be caused. This process can help infrastructure managers prioritize the most significant vulnerabilities, make the best use of investment funding, and take the necessary action to mitigate those vulnerabilities, using scarce resources.

The use of quantitative risk assessment methodologies together with current digital technologies offers great potential to improve the protection of infrastructure. Risk-based approaches enable proactive planning, ongoing monitoring and informed decision making across the infrastructure lifecycle.

1.4 Role of Intelligent Decision Support Systems

The monitoring and management of critical infrastructure are revolutionized through recent advances in Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Big Data Analytics, Geographic Information Systems (GIS), and Digital Twin technologies. All these technologies produce massive amounts of real-time data which, in turn, can be used to identify anomalies, forecast failure, calculate risks, and suggest appropriate response actions.

These technologies combine with knowledge-based reasoning and risk assessment models to create Intelligent Decision Support Systems (IDSS) that help decision makers in complex operational situations. Conventional Decision Support Systems (DSS) cannot handle real-time information, evaluate various risk options, prioritize their response options or provide strategic as well as operational decision making under conditions of uncertainty, whereas IDSSs can.

Implementing intelligent decision support systems can enhance the situational awareness, decrease response time, improve the operational efficiency and increase the critical infrastructure's resilience to multiple hazards.

1.5 Research Gap

Despite the extensive research that has been carried out in the fields of cyber security, disaster management, infrastructure resilience, artificial intelligence, and risk assessment, the studies conducted so far are scattered. The majority of existing research is directed toward a single hazard or a single sector of infrastructure rather than an overall design that can incorporate multiple categories of hazard and place all in one decision-support system.

In addition, very few studies have suggested an intelligent plan that integrates threat identification, vulnerability assessment, artificial intelligence, predictive analysis, risk prioritization and continuous infrastructure monitoring for complete protection of critical infrastructure.

This gap underscores the need for an integrated and intelligent decision-making process that can assist infrastructure managers in identifying risks,

assessing alternative ways to protect infrastructure and enhance infrastructure resiliency in total.

1.6 Research Objectives

This research has two main goals:

To identify the major threats affecting critical infrastructure.

To study the existing risk assessment methods applied to infrastructure protection.

To create a full-fledged Risk Based Protection Framework with an Intelligent Decision Support System.

To incorporate AI and Risk Analytics within infrastructure protection decision-making.

Enhance the resilience of infrastructure by intelligent monitoring and decision support based on evidence.

1.7 Research Contributions

This study has the following contributions:

Introduces a new Integrated Risk-Based Protection Framework for critical infrastructure.

Constructs a conceptual architecture for Intelligent Decision Support System for infrastructure risk management.

Combines various types of threats such as physical, cyber, environment, and operation threats into a single framework.

Showcases the potential of AI for improving infrastructure protection and decision-making.

Gives practical policy, infrastructure and emergency management organizations suggestions.

The paper is organized as follows:

The rest of this paper is organized as follows:

The literature review on critical infrastructure protection, risk assessment and intelligent decision support systems is provided in Section 2.

The research gap is defined and the need for proposed framework is established in Section 3.

The proposed methodology and conceptual framework are described in Section 4.

The architecture of the Intelligent Decision Support System is given in Section 5.

The framework is applied in Section 6 using a representative case study.

The results, the limitations and future research directions are discussed in Section 7.

The paper is then concluded in Section 8 and key contributions are summarized.

2. Literature Review

2.1 Introduction

With modern society's reliance on the interwoven physical and digital infrastructure, Critical Infrastructure Protection (CIP) is one of the most rapidly expanding research topics. Critical infrastructure refers to energy, transportation, healthcare systems, water, communications, financial, oil and gas facilities and emergency services. Disturbances to any of these sectors could have significant consequences for national security, economic development, public safety and environmental sustainability. This has led to an increasing focus on developing intelligent and risk-based solutions to enhance infrastructure resilience and ensure the uninterrupted provision of core services by a government, researchers and infrastructure operators.

The management of critical infrastructure has vastly changed over the last few years, with the introduction of new technologies like Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Big Data Analytics, Geographic Information Systems (GIS), and Digital Twin. They enable real-time monitoring, predictive analysis, automatic risk assessment and intelligent decision making for infrastructure operators to prevent failures and to react effectively to emerging risks.

2.2 Critical Infrastructure Protection

Critical Infrastructure Protection (CIP) is a range of policies, technologies, strategies and practices that protect critical infrastructure against physical, cyber, natural and operational attacks. Traditional protection approaches emphasized mainly physical protection, including surveillance, access control, emergency preparedness planning, and hardening infrastructure. The world of infrastructure protection has, however, undergone a dramatic transformation with the introduction of cyber technologies that are becoming an integral part of physical infrastructures.

Modern critical infrastructure has become an integrated cyber physical system with the integration of operational technologies, information systems, communication networks, and industrial control systems. Therefore, more comprehensive approaches to infrastructure protection which would take into account several

categories of threats, not only a single hazard, have to be developed.

Researchers have stressed that protection cannot be reactive and is best achieved by ongoing monitoring, proactive risk management and adaptation rather than reactive responses after events. Resilience is thus a key goal of infrastructure protection strategies today.

2.3 Risk Based Protection of Critical Infrastructure

Risk Based Protection (RBP) is one of the most accepted approaches for infrastructure security that allows for the prioritization of protection activity based on risk, not on treating all infrastructure equally.

There are three major components that are used when evaluating risk:

- Threat
- Vulnerability
- Consequence

Risk-based protection aims to identify potential threats, consider infrastructure vulnerabilities, estimate risk levels and consequences of disruptive events, and prioritize mitigation options based on overall risk level.

Risk-based methods offer several benefits over traditional protection methods, such as more effective resource allocation, more efficient operations, more preparedness and more resilient infrastructure. The integration of real-time operational data with risk assessment models has additionally been pointed out as an essential step for achieving more precise assessments and enabling organisations to better manage changing threat scenarios quickly.

2.4 Intelligent Decision Support Systems

Decision Support Systems (DSS) have been used for years to support the manager to solve structured and semi-structured decision problems. With the growing complexity of infrastructure, however, Intelligent Decision Support Systems (IDSS) have emerged, which combine Artificial Intelligence (AI), Machine Learning, expert systems, optimization methods, and predictive analytics to assist in complex decision-making in the presence of uncertainty.

Intelligent Decision Support Systems continually draw data from the sensors, monitoring equipment, communication networks, and operational databases to process the data in real time. These systems are able to automatically detect abnormal conditions, analyze various risk scenarios, rank better options for responding, and suggest best protection strategies.

Typically, a Modern Intelligent Decision Support Systems comprise of various functional components like data acquisition, knowledge management, risk assessment, artificial intelligence, optimization algorithms, visualization tools and decision recommendation modules. The integration allows infrastructure managers to gain a better situational awareness, have reduced response times, better optimisation of resources and have higher overall infrastructure resilience.

2.5 Artificial Intelligence in Critical Infrastructure Protection

The course covers all of the previous points and extends them to Critical Infrastructure Protection.All of the above is covered in the course and expanded to Critical Infrastructure Protection.

AI has emerged as one of the most influential technologies aiding infrastructure protection. With AI, intelligent systems can be built to process vast amounts of diverse data, uncover hidden relationships, flag anomalies, foresee infrastructure issues, and suggest suitable mitigation measures.

Machine Learning algorithms are being used more and more in fields like predictive maintenance, cyber intrusion detection, anomaly detection, infrastructure condition assessment and disaster prediction. Furthermore, Deep Learning methods have significantly boosted the ability of infrastructure monitoring systems, particularly in areas such as image recognition, sensor data analysis, and pattern classification.

The use of AI-powered infrastructure protection has shown to be highly effective in enhancing the accuracy of predictions and minimizing operational risks in recent studies. However, researchers also underscore the significance of explainable AI, data quality, transparency, and human oversight to guarantee dependable decision making in critical infrastructure settings.

2.6 Infrastructure Protection by using Digital Twin Technology

Digital Twin technology is a relatively new phenomenon that has become a valuable instrument for monitoring and managing critical infrastructure. A Digital Twin is a virtual model of a physical infrastructure asset that is constantly updated with an operational stream from physical sensors and devices.

Digital Twins combined with Artificial Intelligence can simulate different operational scenarios, anticipate failure of any equipment, analyze emergency situations, and plan maintenance optimally. Digital Twin models give on-going situational awareness and enable decision-makers to consider various response options prior to taking action in the physical infrastructure.

The researchers believe that Digital Twin technology is a key element in the future of smart infrastructure management as it integrates simulation, predictive analysis, and real-time monitoring in one decision support environment.

2.7 Multi-Hazard Risk Assessment

Critical infrastructure faces a myriad of threats, many of which are likely to happen in a cascading or multi-stage fashion. Natural disasters, Cyber attacks, terrorist activity, equipment failure, operational accidents, and human error are all examples of these. Traditional risk assessment models assess these threats individually, while modern infrastructure systems need a multi-hazard risk assessment approach that takes into account interactions among hazards.

Multi-hazard assessment gives infrastructure managers a full picture of infrastructure vulnerabilities and allows for developing a coordinated protection strategy to protect multiple hazards at once. Recent studies have shown that multi-hazard assessment is more effective for an emergency preparedness and infrastructure resilience than single hazard approaches.

2.8 Existing Research Limitations

Although much research has been carried out into the protection of infrastructure, certain shortcomings are apparent in the literature.

Most studies published emphasize cybersecurity and only consider physical and natural hazards to a lesser degree. In a similar manner, some AI research projects highlight predictive modelling without the full inclusion of a risk assessment methodology. Current Decision Support Systems (DSS) tend to focus on operational optimization and have an inadequate mechanism for prioritizing infrastructure risk.

Moreover, very few studies are found to combine AI, Digital Twins, risk assessment, predictive analytics and decision support in an integrated approach to respond to risks of physical, cyber, environmental and operational types.

Lack of uncertainty, explainability, and human decision-making are other restrictions. Decision Support Systems are needed which not only make accurate predictions but also give the reasons for the protection actions recommended to infrastructure managers.

2.9 Summary of Literature Review

The available literature shows that Critical Infrastructure Protection has moved from traditional physical security solutions to intelligent, data-driven, risk-based Critical Infrastructure Protection systems. The use of Artificial Intelligence, Digital Twin, Machine Learning, Internet of Things, and Intelligent Decision Support Systems has greatly improved the monitoring control of infrastructure, predictive maintenance and emergency response.

But the current research is scattered as most studies are individual technology or specific infrastructure sector studies. Comprehensive approaches for the protection of critical infrastructure covering the integration of multi-hazard risk assessment, Artificial Intelligence, Digital Twins and Intelligent Decision Support Systems are still lacking.

The above limitations are addressed in this research by proposing a Risk Based Protection Framework Using Intelligent Decision Support Systems that incorporates threat identification, vulnerability assessment, Artificial Intelligence, predictive analytics and intelligent decision-making that enhance critical infrastructure resilience and protection against a range of threats.

3. Research Gap

The previous section of the literature review has shown that there has been significant development in Critical Infrastructure Protection (CIP), Risk Assessment, Artificial Intelligence (AI), Digital Twin and Intelligent Decision Support Systems (IDSS). They have suggested a variety of approaches

to making infrastructure more resilient, to increasing situational awareness, to predicting infrastructure fail operations, and to aiding emergency response. Notwithstanding the developments, there are still a number of key research gaps to be overcome before a full protection framework in relation to infrastructure becomes possible to implement.

First, a significant share of present investigations are concentrated on singular types of threats, including cyber-attacks, or nature disasters, equipment failures, or terrorism. These studies offer important lessons for particular risk areas but do not usually take into account the inter-relationship of several hazards simultaneously. Modern critical infrastructure is a complex system with numerous interdependencies between physical, cyber, environmental, and operational threats that can lead to cascading failures across infrastructure sectors. Thus, using one-hazard assessment models could result in the mis-estimation of risk and inadequate protection measures.

Second, numerous studies in the literature have been able to apply Artificial Intelligence (AI) and Machine Learning (ML) methods to monitor infrastructure, detect anomalies, predict maintenance needs and predict threats. But, most of these AI-based methods are only about prediction accuracy and not about the whole decision-making process. To date, there are no models that offer structured suggestions to infrastructure managers on how to choose mitigation strategies, where to allocate resources, or how to prioritize protection strategies when faced with uncertainty.

Thirdly, Digital Twin technology has become a potential platform for infrastructure monitoring and simulation. Digital Twins are used to visualize infrastructure in real time and to support predictive maintenance by continuous data synchronization. However, most existing Digital Twin applications are focused on asset monitoring and operational performance, and there are relatively few studies that consider Digital Twin and Risk Assessment Methods and Intelligent Decision Support Systems for strategic protection of infrastructure.

Another important limitation found in the literature is that there is no integrated decision making model that incorporates the identification of threats, vulnerability assessment, risk analysis, Artificial Intelligence, predictive analysis and decision support into a single system. Current Decision Support Systems are generally detached from risk assessment systems and therefore are not able to give a comprehensive recommendation both on an operational efficiency and on an infrastructure security level.

Moreover, many previous studies are limited to certain application areas such as power systems, transportation network, healthcare facilities and water distribution systems. Their proposed solutions are therefore only limited applicable to various infrastructure domains. A generic and flexible approach to support multiple critical infrastructure sectors is not well-studied.

Given the identified limitations, there is a clear need for a comprehensive Risk Based Protection Framework Using Intelligent Decision Support Systems, which is a unified, cohesive framework that encompasses multi-hazard risk assessment, Artificial Intelligence, Digital Twin technology, predictive analytics and intelligent decision-making. This holistic approach would help the infrastructure managers to discover new threats, assess the infrastructure vulnerabilities, prioritize mitigation plans, allocate resources optimally and increase the overall infrastructure resilience against various physical, cyber, environmental and operational risks.

Based on the identified research gaps, this research introduces an integrated Intelligent Decision Support Framework for risk-based critical infrastructure protection, which aims to help create more resilient, adaptive and evidence-based critical infrastructure security management.

4. Proposed Framework and Methodology

4.1 Overview

This research suggests a Risk Based Protection Framework Using Intelligent Decision Support Systems (IDSS) for critical infrastructure against multiple threats. The framework brings together (Risk Assessments, Artificial Intelligence (AI), Digital Twin technology, Internet of Things (IoT), predictive analytics, and intelligent decision-

making) into a single architecture. The proposed framework goes beyond traditional protection strategies that address individual hazards and technologies, by continually gathering operational information, identifying emerging threats, evaluating infrastructure vulnerabilities, prioritizing the risks, and proposing appropriate protection strategies.

The proposed framework is aimed at strengthening the infrastructure's resilience by facilitating proactive decision-making, and not reactive. It enables the infrastructure manager to rapidly respond to physical, cyber, environmental and operational threats, giving them real-time situational awareness, evidence-based recommendations and continuous monitoring.

4.2 Framework Objectives

The proposed framework has the following objectives:

- To recognize and categorize threats to critical infrastructure.
- To perform a structured approach to assessing vulnerabilities in infrastructure.
- To assess the risk and impact of various threat situations.
- To incorporate Artificial Intelligence in predictive risk analysis.
- To enable smart infrastructure management decision making.
- To prioritize measures for protection according to a calculated risk level.
- To continuously track the performance of infrastructure and real-time updating the risk assessments.
- To enhance the resilience and continuity of infrastructure.

4.3 Overall Framework Architecture

The proposed framework has seven interconnected and supporting steps in the protection of intelligent infrastructure.

Phase 1: Data Acquisition

This is the first stage, which involves gathering information from a number of sources, such as:

- IoT sensors
- SCADA systems
- CCTV surveillance
- GIS databases
- Weather monitoring systems
- Historical incident databases
- Infrastructure inspection reports
- Cybersecurity monitoring systems

Collected data serve as the basis for the following risk analysis and intelligent decision making.

Phase 2: Threat Identification

Once the data have been collected, possible threats to the infrastructure are being identified and classified.

Threat categories include:

- Natural hazards
- Floods
- Earthquakes
- Hurricanes
- Wildfires
- Physical threats
- Terrorism
- Sabotage
- Theft
- Vandalism
- Cyber threats
- Malware
- Ransomware
- Network intrusion
- SCADA attacks
- Operational threats
- Equipment failure
- Human error

It involves a disruption in the supply chain.

Each threat identified is assessed based on its nature, likelihood and likely impact on the operations of the infrastructure.

Phase 3: Vulnerability Assessment

Threats identified, then infrastructure vulnerabilities are assessed.

The vulnerability assessment is carried out on:

- Infrastructure age
- Structural condition
- Cybersecurity maturity
- Physical security measures
- Maintenance history
- Operational reliability
- Redundancy level

A vulnerability score quantifies the susceptibility of each infrastructure component to threats that are identified.

Phase 4: Risk Assessment

The fourth phase is an estimate of the overall infrastructure risk.

The proposed framework evaluates the risk in the following three major components:

Risk = Threat x Vulnerability x Consequence

Where:

Threat = the likelihood of occurrence.

Vulnerability is a weakness in infrastructure.

Consequence – potential operational, financial, environmental and human impacts.

There are three categories of risk values:

- Very Low Risk
- Low Risk
- Medium Risk
- High Risk
- Critical Risk

These categories help decision makers prioritize mitigation strategies.

Phase 5: Artificial Intelligence-Based Risk Prediction

The proposed framework uses Artificial Intelligence for enhancing the accuracy of the prediction.

Analyse using Machine Learning algorithms:

- Historical incidents
- Sensor data
- Environmental conditions
- Infrastructure performance
- Security events

AI models detect abnormal patterns, forecast potential infrastructure failures, assess future risks, and continually adjust infrastructure risk levels.

AI can provide predictive risk analysis, which is dynamic and adaptive, unlike static risk prediction techniques.

Phase 6: Intelligent Decision Support System

The Intelligent Decision Support System is the main element of the proposed framework.

The Decision Support System then works with user-specified protection rules, optimization algorithms and expert knowledge to analyze various protection options after receiving the calculated risk information.

Recommendations such as:

- Infrastructure shutdown
- Equipment isolation
- Preventive maintenance
- Resource allocation
- Emergency response activation
- Cybersecurity countermeasures
- Evacuation planning
- Recovery planning

All of the above issues (criticality, resources, operational priorities, risk acceptance) are taken into account in the decision making process to recommend the most suitable mitigation action.

Phase 7: Ongoing monitoring and feedback

The protection of infrastructure is not a "one-and-done" kind of operation.

Thus, the last stage of monitoring is an ongoing process:

- Infrastructure health
- Environmental conditions
- Cybersecurity events
- Operational performance
- AI prediction accuracy

The system is continuously fed back on new operational data, enabling the automatic updating of risk assessments and better decision making in the future.

This adaptive infrastructure protection mechanism provides protection when operational conditions are changing.

The proposed framework offers several benefits.The proposed framework has many advantages.

The proposed framework has several benefits over the existing frameworks.

Firstly, it brings together multiple threats within a single decision making environment, as opposed to cyber, physical and environmental threats being considered separately.

Second, the framework integrates Artificial Intelligence, risk assessment and Intelligent Decision Support Systems in a single architecture which can support complex infrastructure protection decisions.

Thirdly, constant monitoring enables infrastructure managers to identify abnormal conditions in time and take the necessary measures to mitigate before the major failure happens.

Fourthly, the framework enhances the use of resources by prioritizing mitigation actions based on the calculated risks, not subjective judgements.

Lastly, the proposed architecture is versatile and can be implemented in different sectors of critical

infrastructure such as transportation networks, healthcare centers, energy networks, water distribution systems, airports, seaports, oil and gas installations, and smart cities.

4.5 Methodology

The method used in this study is Design Science Research (DSR), because the basic ideas for this study are to design and test a new model for protecting critical infrastructure. The methodology consists of the following stages:

1.Problem Identification: Examine the problems of protecting critical infrastructure against multi-hazard threats.

2.Literature Review: Study recent literature on CIP, risk assessment, A.I., Digital Twins and Intelligent Decision Support Systems.

3.Framework Design: Create a comprehensive Risk-Based Protection Framework that incorporates threat identification, vulnerability assessment, AI-based threat prediction, and decision support.

4.Conceptual Validation: Check how the framework will compare with other approaches and determine if it can fill in the research gaps that were found.

5.Case Study Application: Show how the framework is applicable in a realistic scenario for critical infrastructure.

6.Discussion and Evaluation: Discuss the pros, cons, and possible improvements of the proposed framework.

4.6 Summary

The Risk Based Protection Framework is an integrated and intelligent solution for protecting critical infrastructure from physical, cyber, environmental and operational threats. The framework can be implemented using a structured risk assessment combined with Artificial Intelligence and Intelligent Decision Support Systems, which will increase the awareness of the situation, assist in evidence-based decision making, and strengthen the resiliency of infrastructure. The detailed architecture of the Intelligent Decision Support System is provided and the interaction of its components to support real-time infrastructure protection is explained.

5. Intelligent Decision Support System Architecture

5.1 Overview

The Intelligent Decision Support System (IDSS) is the key element to the proposed Risk Based Protection Framework. It is intended to help infrastructure managers, emergency responders and decision makers to detect threats, assess risks, choose mitigation options and enable timely decisions. The proposed IDSS will combine Artificial Intelligence (AI), Machine Learning (ML), Internet of Things (IoT), Digital Twin technology, and real-time monitoring to offer dynamic and intelligent recommendations that go beyond the capabilities of traditional Decision Support Systems (DSS), which are mostly based on pre-defined rules and historical data.

The architecture described will allow infrastructure data to be continuously collected and analyzed from various sources. The system uses predictive analytics and a structured risk assessment to identify unusual circumstances, assess future risks, prioritize threats, and suggest the most suitable protection measures. This comprehensive approach leads to better decision-making, faster response times, and heightened critical infrastructure resiliency.

5.2 Architecture of the Proposed Intelligent Decision Support System

In this section, the design of the proposed intelligent decision support system is presented.In this section, the architecture of the proposed Intelligent Decision Support System (IDSS) is presented.

The proposed Intelligent Decision Support System is composed of seven layers with each layer having a specific role to play in the decision making process. These layers form a complete solution to monitor infrastructure conditions, analyze risks, make intelligent recommendations and assure continuous protection.

This is the layer where the data is gathered. The layer in which data is collected.

The Data Acquisition Layer collects data from different internal and external sources to get operational data. These data are the basis of intelligent analysis and decision.

The system is given data by:

- IoT sensors
- SCADA systems
- CCTV surveillance

Geographic Information Systems (GIS)
- Weather monitoring stations
- Industrial control systems
- Network security devices
- Historical incident databases
- Infrastructure inspection reports
- Maintenance records

This layer is responsible for collecting, synchronizing and doing some basic data pre-processing of the huge amount of data generated by infrastructure environments, and then transferring it to the higher processing layers.

Data Management Layer: Layer 2 of the stack.

The Data Management Layer manages, organizes and stores all infrastructure data collected.

It has the following main duties:
- Data cleaning
- Data validation
- Data integration
- Data normalization
- Database management
- Historical data storage

The aim of this layer is to provide high quality and reliable information for subsequent analysis. Data inaccuracies or gaps can have a significant impact on the performance of AI prediction models and risk assessment procedures.

The third layer is the Artificial Intelligence and Analytics Layer.The third layer is the Artificial Intelligence and Analytics Layer.

The Artificial Intelligence Layer is the intelligence of the architecture proposed.

This layer implements sophisticated computational methods such as:
- Machine Learning
- Deep Learning
- Predictive Analytics
- Pattern Recognition
- Anomaly Detection
- Classification Algorithms

AI models detect abnormal behaviour, estimate degradation of infrastructure, highlight emerging threats, predict equipment failures and forecast future risks, all using historical and real time operational data.

AI systems can provide predictive monitoring capabilities, forecasting the state of infrastructure before a failure by analyzing historical data and patterns.AI can be used for predictive monitoring, which uses historical data and patterns to anticipate infrastructure conditions before failures occur.

Layer 4: Risk Assessment Layer

The Risk Assessment Layer analyzes infrastructure risks by utilizing information created by the AI engine.

There are three main parts of risk evaluation:
- Threat Assessment
- Vulnerability Assessment
- Consequence Analysis

The identified threats are analysed based on the following:
- Probability of occurrence
- Infrastructure vulnerability
- Potential operational impact
- Economic consequences
- Environmental consequences
- Human safety implications

The system uses these based parameters to determine an overall risk score for each infrastructure asset.

The risks calculated are grouped into:
- Very Low Risk
- Low Risk
- Moderate Risk
- High Risk
- Critical Risk

These categories help decision makers prioritize mitigation activities and use available resources efficiently.

Layer 5: Knowledge Base

All expert knowledge is stored in the Knowledge Base, which can be used for smart decisions.

It includes:
- Infrastructure protection policies
- Risk assessment standards
- Emergency response procedures
- Historical incident reports
- Best practice guidelines
- Infrastructure operating procedures
- Maintenance strategies

The Knowledge Base is continually updated with new operational experiences, incident reports and expert recommendations.

The Intelligent Decision Support System can continuously learn and build up knowledge, which can further enhance its recommendation results.

Layer 6: Decision Support Engine

The most important part of the proposed architecture is the Decision Support Engine.

This engine integrates:

- AI prediction results
- Risk assessment outcomes
- Knowledge Base information
- Infrastructure operational status

It performs optimization algorithms & expert decision rules to consider various response options and then recommends the most suitable protection method.

Possible recommendations include:

- Infrastructure shutdown
- Equipment isolation
- Preventive maintenance
- Cybersecurity response
- Emergency evacuation
- Resource reallocation
- Backup system activation
- Infrastructure inspection
- Incident investigation

The proposed approach is not intended to make decisions for humans, but to assist in decision-making by presenting evidence-based recommendations based on it.

Layer 7: Visualization and User Interface Layer

The last layer offers an interactive interface, where infrastructure managers will monitor system status and be given decision recommendations.

The dashboard presents:

- Infrastructure health indicators
- Risk levels
- Threat alerts
- Infrastructure location maps
- AI prediction results
- Recommended mitigation strategies
- Incident history
- Performance indicators

Visualization tools help to make complex analytical data easier to understand.

Infrastructure managers are able to compare various response scenarios to inform decisions for operations.

The operational workflow of the intelligent decision support system is described in this section.In this section, the operational workflow of the intelligent decision support system is described.

The Intelligent Decision Support System is intended to be implemented in a continuous manner of decision-making.

First, data on the operation of the infrastructure systems is taken from several infrastructure monitoring systems.

These data are handled and stored in the Data Management Layer.

This information is then analyzed by AI algorithms to detect abnormal conditions and anticipate possible problems.

The Risk Assessment Layer assesses risks to infrastructure, and is based on threat probability, infrastructure vulnerability, and consequence analysis.

The Decision Support Engine then compares a multitude of mitigation strategies according to predetermined decision rules and optimization methods.

Finally, protection measures are displayed to infrastructure managers using an interactive protection dashboard.

Once the system is put in place, new operational data is continually gathered and fed into the system and the complete decision making cycle can repeat automatically.

This ongoing feedback system allows adaptive infrastructure protection in dynamic operational conditions.

The proposed Intelligent Decision Support System offers several benefits.The following are some of the benefits of the proposed Intelligent Decision Support System.

The proposed architecture offers a number of key benefits over traditional infrastructure management strategies.

First, it helps to monitor the infrastructure in real-time by collecting and analyzing data continuously.

Secondly, using Artificial Intelligence, it can predict future infrastructure failures with greater accuracy, pinpointing hidden patterns.

Third, structured risk assessment enables objective prioritization of protection strategies based on the criticality of infrastructure.

Fourth, decision-makers are provided with intelligent recommendations and not based on subjective judgement, which will in turn enhance the quality and consistency of operational decisions. Fifth, by combining several technologies into one architecture, infrastructure resilience against physical, cyber, environmental and operational threats is improved.

Last but not least, the modular concept of the proposed system enables adaptation in a variety of infrastructure sectors such as energy systems, transport systems, medical facilities, water supply, airport, oil and gas facilities, telecommunications, and smart cities.

5.5 Summary

The suggested Intelligent Decision Support System architecture offers a thorough basis to support risk-based protection of critical infrastructure. The system incorporates Artificial Intelligence, risk assessment, expert knowledge, predictive analysis, and ongoing monitoring, which boosts its decision-making capabilities and fortifies infrastructure resilience. The proposed architecture is different from conventional decision support systems in that it provides for adaptive, real time and evidence-based recommendations to help infrastructure managers respond to the varied threats. The resulting architecture is the technological backbone of the proposed architecture and is used as the basis for the practical application outlined in the following case study.

6. Case Study / Application Scenario

6.1 Introduction

In order to illustrate the effectiveness and applicability of the proposed Risk Based Protection Framework Using Intelligent Decision Support Systems (IDSS), a fictional case study of a large public hospital as critical infrastructure is presented. Hospitals are among the most important assets of today's society and are expected to continue offering the care and services necessary to healthcare, and as part of response and relief efforts in case of natural disasters, pandemics or security incidents. They are reliant on a variety of interdependent systems, such as electrical power, water, communications, medical systems, HVAC systems, information technology, and emergency backup systems. These systems are vital to the safety of patients, care of health services and public confidence and any disruption can have a significant impact on these.

The case study is used to demonstrate the application of the proposed framework to detect threats, evaluate risks, prioritise mitigation approaches and provide intelligence in the support of infrastructure managers.

6.2 Description of the Critical Infrastructure

The chosen infrastructure is a 500 bed tertiary care hospital in a metropolitan area. The hospital offers services at its emergency center, surgical and intensive care units, diagnostic imaging center as well as specialized treatment units. It is in use all year long and is a mix of physical infrastructure and digital technologies.

The critical assets of the hospital are:

- Electrical power distribution system
- Emergency diesel generators

Heating, Ventilation and Air Conditioning (HVAC) systems

- Medical gas supply systems
- Water supply and storage systems
- Hospital Information System (HIS)
- Electronic Medical Records (EMR)
- Medical imaging equipment
- Communication networks

These are also called IP cameras.These are also known as CCTV and access control systems.

These systems are very interdependent and failure of the one system could be a failure of multiple hospital systems.

6.3 Threat Identification

The proposed framework identifies potential threats to the operations of hospitals and classifies them into four main categories.

Natural Threats

Natural hazards include:

- Flooding
- Earthquakes
- Severe storms
- Extreme temperatures

These events can cause property damage, utility service disruptions and access to the hospital could be limited when an emergency arises.

Physical Threats

Physical threats include:

- Terrorist attacks

- Unauthorized access

Theft of medical equipment.

- Vandalism
- Fire incidents

These threats can impact upon hospital operations and have the potential to become a risk to patient safety.

Cyber Threats

Medical data is of great value and healthcare organizations are now the regular targets of cyber-attacks.

The potential threats to the cyber domain are:

- Ransomware attacks
- Malware infections
- Data breaches
- Denial-of-Service (DoS) attacks
- Insider threats
- Unauthorized network access

Such strikes can have a fatal impact on hospital information systems and cause delays for the delivery of vital medical care.

Operational Threats

Operational risks include:

- Equipment failure
- Human error
- Power outages
- Network failures
- HVAC malfunction
- Generator failure

These failures can affect the capacity of the hospital to provide uninterrupted health services.

6.4 Risk Assessment

The proposed framework then conducts a structured risk assessment after threat identification.

Three parameters are used to assess each identified threat:

- Threat Probability
- Infrastructure Vulnerability
- Consequence Severity

Overall risk level is calculated as:

Risk = Threat x Vulnerability x Consequence

A ransomware attack on the HIS could have, for instance:

- High probability
- Medium vulnerability
- Critical operational consequences

As such, this threat is considered a High Risk threat and should be addressed immediately.

Likewise, a temporary network disconnection could be of less consequence and be assigned a Moderate Risk rating.

This risk prioritization helps hospital management target their resources to the highest risk vulnerabilities.

6.5 Artificial Intelligence Based Risk Prediction

The Artificial Intelligence module uses sensor data, network monitoring systems, maintenance databases, and historical data of incidents to constantly analyze operational data.

Machine Learning algorithms are used to watch:

- Equipment performance
- Network traffic
- Environmental conditions
- Energy consumption
- Medical equipment utilization
- Generator operating parameters

If unexpected temperature readings are found in the electrical distribution room in the hospital, then what? The AI model recognizes this deviation from normal operating conditions and forecasts a higher likelihood of electrical equipment failures.

As soon as the failure is imminent, the system will generate an early warning, so that maintenance staff can check the equipment and stop the service from being interrupted.

Likewise, the AI engine can automatically detect abnormal network traffic that may mean ransomware activity and alert cybersecurity personnel at the moment.

6.6 Intelligent Decision Support Process

The Intelligent Decision Support System analyzes various response options after risk prediction.

In the ransomware case, the recommended steps are:

Segregate infected areas of the network.

- Turn on cybersecurity incident response processes.

Restore data from secure backups.

Report to hospital security Computer.

- Increase network monitoring.

Ensure the maintenance of critical clinical services using alternative arrangements.

If there is an electrical system failure, the system suggests:

- Activate emergency generators.
- Transfer critical loads to backup power.
- Dispatch maintenance personnel.
- Contact hospital EMS.

Continue to monitor electrical parameters.

The recommendations are prioritised based on the assessed risk and the need and criticality of the affected services of the hospital.

These recommendations can be viewed in the system dashboard before making any operational decisions as an infrastructure manager.

6.7 Expected Outcomes

There are a number of operational advantages associated with the application of the proposed framework.

First, continuous monitoring allows for early detection of abnormal conditions with infrastructure before they become serious failures.

Secondly, AI prediction can optimize maintenance scheduling and minimize unplanned equipment downtime.

Third, structured risk assessment enables financial and technical resources to be allocated to critical infrastructure based on objective assessment, not on subjective opinion, within the hospital.

Fourth, intelligent decision support minimises response time in case of emergency, as it offers pre-defined evidence-based recommendations.

Last but not least, the combination of physical security, cyber security, operational monitoring and risk assessment in a single holistic approach enhances the hospital's overall resilience to various threats.

6.8 Practical Implications

This case study is a healthcare facility but the framework suggested is flexible enough to apply to a wide range of critical infrastructure categories.

It can be used for:

- Electrical power plants
- Water treatment facilities
- Airports
- Seaports
- Railway transportation systems
- Oil and gas facilities
- Smart cities
- Telecommunications infrastructure
- Government buildings
- Industrial manufacturing plants

The particular threat models, operating conditions and infrastructure elements must be tailored for each application domain.

6.9 Summary

This case study is a demonstration of the application of the proposed Risk Based Protection Framework Using Intelligent Decision Support Systems in a real world critical infrastructure setting. The framework incorporates multi-hazard threat identification, structured risk assessment, Artificial Intelligence, predictive analytics, and intelligent decision support, offering a proactive approach to infrastructure management and improving operational resilience. The hospital case study is used here to illustrate the approach, but the methodology is applicable to a variety of critical infrastructure sectors and offers a practical basis for enhancing infrastructure protection and decision making in the face of complex and dynamic conditions.

7. Discussion

7.1 Introduction

The growing complexity of today's critical infrastructure has introduced many challenges for critical infrastructure operators, emergency managers, and public policy makers. Existing protection methods, for which the core focus is primarily on periodic inspection, manual risk assessment and reactive incident management, are no longer adequate to respond to an ever-changing threat landscape. Today, critical infrastructure also faces multiple interrelated threats such as cyber-attacks, natural disasters, terrorist threats, equipment failure or malfunction, and human error. These risks are likely to be happening at once and can lead to chain reactions of failures in various sectors of the infrastructure.

To overcome these challenges, this study introduced a Risk-Based Protection Framework Using Intelligent Decision Support Systems (IDSS) that combines the technologies of Artificial Intelligence (AI), structured risk assessment, Digital Twin concepts, predictive analytics, and intelligent decision support in a single framework. The framework proposed is discussed in this section, followed by a discussion on its practicality, a comparison of the proposed framework with existing approaches, challenges in implementing

the proposed framework, and future research directions.

7.2 The significance of the proposed framework.

An important innovation of the proposed framework is that it brings together various technologies in a single decision making architecture. The framework is not just about recognizing threats and assessing vulnerabilities but also about predicting threats, prioritizing risks, and making decisions—all in an ongoing cycle, rather than individual components tackled in isolation as with traditional infrastructure protection strategies.

This integration helps infrastructure managers transition from merely reacting to incidents to proactively managing risks. By addressing threats that are becoming apparent, forecasting which threats may fail, and taking preemptive measures before operational disruptions turn into large-scale incidents, rather than reacting to failures, a decisionmaker can minimize the risks.

Moreover, the framework advocates for a quantitative risk assessment and intelligent analytical models that help in evidence-based decision making. This will minimize subjectivity in decision making and increase the consistency and transparency of operational decisions.

7.3.1. AI in business

The proposed framework has one of the most important components: Artificial Intelligence. Machine Learning algorithms enhance the ability of infrastructure managers to process massive amounts of data, including operational, sensor, communication, and maintenance data, to make sense of it.

The adoption of AI offers several benefits in terms of its operation:

- Early detection of abnormal conditions of infrastructure.
- Ability to anticipate equipment failure and prevent them.
- Ongoing infrastructure health evaluation.
- Automated detection of cyber risks.
- Enhanced emergency response plans.
- Learning from past incidents.

Unlike the traditional monitoring system which only captures and shows the current operational condition, AI learns continuously from the past and current data, making predictions about the behaviour of infrastructure more accurate.

AI models are also reliant on the availability of high-quality data, though. Prediction accuracy may be limited if sensors do not calibrate properly, or if there are data gaps or inaccuracies in the operational record. Hence, the need for data governance and quality assurance to ensure accurate AI implementation.

7.4 Contribution of Intelligent Decision Support Systems

The proposed Intelligent Decision Support System is a combination of the conventional Decision Support System with a level of Artificial Intelligence, optimization techniques, expert knowledge, and structured risk assessment and placed under a common architecture.

The system is intended to be used as an intelligent support tool for the decision maker, not as a replacement, and is designed to assess several protection options, and suggest the most suitable mitigation measures based on infrastructure characteristics and risk assessment.

This is especially important when facing emergency situations in which quick decisions must be made. Infrastructure managers often face the time constraint and lack of information. The proposed IDSS provides objective analytical models to help the decision-maker structure information available, assess the feasibility of alternatives, and make priority recommendations.

7.5 Extension to Other Systems

The literature review showed that most of the previous research is focused on specific research fields like Artificial Intelligence, Digital Twins, cyber security, disaster management or infrastructure monitoring. While these studies provide valuable knowledge, they tend to focus on a single dimension of protection of infrastructure.

The proposed framework has several points of departure from the other approaches.

First, it takes a multi-hazard approach, taking into account both physical, cyber, environmental and operational hazards together. This is due to the inter-dependency of current infrastructure systems, where system failures in one domain can cause failures in another.

Secondly, the framework incorporates a structured risk assessment and intelligent decision support. Most of the studies use AI as a prediction tool and do not use the prediction outcomes in a comprehensive decision-making process for both mitigation planning and resource allocation.

Third, the framework is sector neutral and adaptations to a wide range of infrastructure sectors like health care, transport, energy, water, telecommunications, airports, industrial facilities etc. are possible. The flexibility also makes it more versatile in various operational scenarios.

7.6 Practical Implications

There are some practical implications of the proposed framework for the infrastructure operators and the policymakers.

The framework can be leveraged by infrastructure managers to schedule maintenance activities based on risk calculations, which will aid in more efficient operations and maintenance cost reduction. Continuous monitoring helps to detect degradation of infrastructure early so that preventive maintenance can be undertaken before it reaches a catastrophic level.

The framework can be used to enhance preparedness by emergency management organisations to assess multiple scenarios of emergencies and to create evidence-based emergency response plans. The framework can also be used by the various government sectors tasked with national infrastructure protection to assist with strategic planning, investment prioritization and assessment of resilience.

In addition, as cybersecurity monitoring is integrated with physical infrastructure protection, it creates a more holistic security approach that can tackle new cyber-physical threats.

7.7 Limitations of the Proposed Framework

The proposed framework has a number of benefits, but some limitations should be recognised.

The framework has been introduced as a conceptual model featuring a representative case study. The deployment needs to be validated on real-world infrastructure data sets at large scale within operational infrastructure environments.

Secondly, AI models need to have a lot of good historical and operational data. For organizations facing a lack of monitoring, prediction accuracy will be lower until more data is collected.

Third, the proposed architecture might be very costly when it comes to the hardware, including sensors, communication infrastructure, cloud computing resources, and cyber security technologies. In smaller companies, there may be budget limitations for deployment, for example.

Last but not least, it is essential to align the efforts of infrastructure engineers, cybersecurity experts, emergency managers and policy makers to ensure successful implementation. Organizational resistance to technological change can also be a factor in adoption.

7.8 Future Research Directions

There are several avenues to pursue in future studies with regards to the proposed framework.

Advanced Deep Learning algorithms in future studies will enhance the accuracy of predictions in the most dynamic operational conditions. The use of Adaptive Decision Making in the context of rapidly changing emergency situations could also be considered through the Reinforcement Learning approach.

The introduction of blockchain technology could improve data integrity, data sharing and cybersecurity in distributed infrastructure systems.

The other promising research lines are the integration of digital twin technology in a more comprehensive way, which has led to the creation of completely synchronized environments for virtual infrastructure that can support real-time simulation and optimization.

Further validation should also be conducted through several real-world case studies, in various infrastructure sectors such as transportation networks, energy systems, smart cities, airports and water distribution systems. To complement the usefulness of the proposed framework, a comparison of the performance of the proposed framework with other approaches to infrastructure management would be useful.

7.9 Summary

The discussion highlights that the proposed Risk Based Protection Framework Using Intelligent Decision Support Systems provides a comprehensive and practical solution to enhance CI resilience. The framework leverages Artificial

Intelligence, structured risk assessment, predictive analytics, and intelligent decision support to improve situational awareness, support evidence-based decision-making, and enable proactive infrastructure management. While there are still issues concerning data quality, implementation costs and organizational acceptability, the proposed framework offers a solid foundation for further research and implementation. It is flexible and has been designed to work across a variety of sectors making it suitable for use in a wide variety of critical infrastructure applications, which helps to ensure more resilient, secure, sustainable infrastructure systems to combat ever-growing and interconnected threats.

8. Conclusion and Future Work

8.1 Conclusion

Critical infrastructure serves as the backbone of today's society and provides the essential infrastructure for energy, healthcare, transportation, water supply, telecommunications, financial systems, and emergency response. As physical infrastructure is being woven into the fabric of digital technologies, this has enabled a significant boost in operational efficiency, but it's also created new vulnerabilities. Infrastructure faces a variety of threats today, ranging from cyber attacks to natural disasters, physical attacks to equipment failures, and human mistakes. These problems are continuously changing and demand protection strategies that are intelligent, adaptable and risk-based, going beyond traditional security methods.

This study suggested a Risk-Based Protection Framework Using Intelligent Decision Support Systems (IDSS) for the improvement of the resilience and security of critical infrastructure. The framework proposed combines all the elements of structured risk assessment, Artificial Intelligence (AI), Machine Learning (ML), Digital Twin concepts, predictive analytics and intelligent decision support into a single architecture. The framework allows infrastructure managers to: continually monitor infrastructure conditions, identify emerging threats, assess vulnerabilities, prioritize risks, and provide evidence-based mitigation measures.

The literature review showed that, while there have been substantial advances in the protection of infrastructures, current research in the field is still disjointed. The majority of past research deals with particular issues including cybersecurity, disaster management, AI prediction mechanism or Digital Twin applications. There is limited research available that offers a comprehensive framework combining multi-hazard risk assessment with intelligent decision support for critical infrastructure protection. This research gap was identified and thus served as a motivator for the creation of the proposed framework.

The methodology proposed is systematic risk management process which includes the following stages: data collection, threat identification, vulnerability assessment, risk analysis, AI-based threat prediction, intelligent decision support, and continuous monitoring. The proposed framework merges with the traditional infrastructure protection methods mainly based on periodic inspection and manual decision-making, while the former methods can realize continuous analysis of real-time operation information and realize proactive risk management.

The Intelligent Decision Support System is the backbone of the framework, combining AI-driven predictions, a structured risk assessment process, and expert knowledge to offer infrastructure managers optimised protection recommendations. The system does not take the place of human decision-makers; instead its output complements their decisions, providing timely, consistent and evidence-based recommendations that assist effective operational planning and emergency response.

The hospital case study illustrated the effectiveness of the proposed framework in a realistic critical infrastructure setting. The framework was a great success in creating a representation of how a multi-hazard threat can be identified, assessed, prioritized and mitigated with intelligent decision making. While the case study was based on the healthcare sector, the proposed framework could be easily extended to other critical sectors like power systems, transportation network, airports, water treatment, telecommunication, oil and gas plants, or smart city.

This study adds to the critical infrastructure protection research by providing an integrated and

scalable framework that integrates modern intelligent technologies and existing risk management concepts. The intended solution will make infrastructure more resilient, increase situational awareness, facilitate proactive maintenance, and help to make better decisions in the face of uncertainty and fast changing operations.

8.2 Future Work

While the proposed framework offers an overall conceptual approach to the protection of critical infrastructure there is a number of opportunities for further research and development in practice.

Future research should bear on the database validation of the framework through real-world operational data collected from various types of critical infrastructures. The piloting of the framework on a large scale in sectors like energy, transportation, healthcare, water management etc will give valuable insight into the effectiveness and scalability of this framework as well as its operational performance in real time.

Second, the more advanced Artificial Intelligence (AI) techniques can be used to enhance prediction accuracy and decision making. Threat detection, infrastructure forecasting, and automated response planning could all be greatly improved by Deep Learning, Reinforcement Learning, Explainable Artificial Intelligence (XAI), and Generative AI, while also providing greater transparency and user trust.

Thirdly, future research should explore how Digital Twin technology can be a fully synchronised virtual representation of physical infrastructure. By simulating emergency scenarios, assessing alternative protection measures, planning maintenance activities, and planning operations, Real-time Digital Twins could help infrastructure operators make decisions in advance of implementation, in the real world.

Another promising path could be integrating blockchain technology to enhance cyber security, data integrity, secure information sharing, and access control processes across multiple infrastructure stakeholders. Distributed infrastructures with multiple organizations sharing sensitive operational information may benefit from blockchain-based solutions to enhance trust.

The proposed framework could also be expanded in future to include more advanced optimization algorithms for resource allocation, emergency logistics, and resilience planning. Satisfying multiple requirements such as infrastructure operational performance, economic cost, environmental protection, and facility security can be achieved through the aid of multi-objective optimization methods.

Finally, comparative analyses need to be done to compare the proposed framework with the existing infrastructure protection models according to the same performance indicators, including prediction accuracy, response time, decision quality, operational cost, improvement of resilience and system reliability etc. These assessments could deliver more empirical evidence of the framework's effectiveness and encourage governments, policy makers and infrastructure operators to embrace it.

Finally, the suggested Risk-Based Protection Framework Using Intelligent Decision Support Systems offers a solid basis for future protection of critical infrastructure. As technology advances and becomes a reality, the framework can evolve to enable resilient, intelligent, and sustainable infrastructure systems to meet the future's growing complexity.

8 References

[1] M. Bruneau et al., "A Framework to Quantitatively Assess and Enhance the Seismic Resilience of Communities," Earthquake Spectra, vol. 19, no. 4, pp. 733–752, 2003.

[2] M. Omer, A. Mostashari, and M. Nilchiani, "Measuring the Resilience of the Critical Infrastructure Systems," Systems Engineering, vol. 12, no. 4, pp. 341–360, 2009.

[3] E. Zio, "Challenges in the Vulnerability and Risk Analysis of Critical Infrastructures," Reliability Engineering & System Safety, vol. 152, pp. 137–150, 2016.

[4] P. Pederson et al., Critical Infrastructure Interdependency Modeling: A Survey, Idaho National Laboratory, USA, 2006.

[5] R. Setola, V. Rosato, E. Kyriakides, and E. Rome, Managing the Complexity of Critical Infrastructures, Springer, 2016.

[6] S. M. Rinaldi, J. P. Peerenboom, and T. K. Kelly, "Identifying, Understanding and Analyzing Critical Infrastructure Interdependencies," IEEE Control Systems Magazine, vol. 21, no. 6, pp. 11–25, 2001.
[7] A. Ross, NIST Cybersecurity Framework Version 2.0, National Institute of Standards and Technology (NIST), 2024.
[8] ISO 31000:2018, Risk Management—Guidelines, International Organization for Standardization, Geneva, Switzerland, 2018.
[9] IEC 62443, Industrial Communication Networks – IT Security for Industrial Automation and Control Systems, International Electrotechnical Commission, 2023.
[10] A. Alderson, Critical Infrastructure: Reliability and Vulnerability, Springer, 2021.
[11] E. Zio, The Future of Risk Assessment, Elsevier, 2018.
[12] T. Aven, Risk Assessment and Risk Management, Springer, 2016.
[13] R. Yager and J. Kacprzyk, The Ordered Weighted Averaging Operators, Springer, 1997.
[14] D. Kahneman, Thinking, Fast and Slow, Farrar, Straus and Giroux, 2011.
[15] S. Russell and P. Norvig, Artificial Intelligence: A Modern Approach, 4th ed., Pearson, 2021.
[16] I. Goodfellow, Y. Bengio, and A. Courville, Deep Learning, MIT Press, 2016.
[17] K. Murphy, Machine Learning: A Probabilistic Perspective, MIT Press, 2012.
[18] F. Chollet, Deep Learning with Python, 2nd ed., Manning Publications, 2021.
[19] T. Gruber, "Artificial Intelligence and Intelligent Decision Support Systems," AI Magazine, vol. 44, no. 1, pp. 5–18, 2023.
[20] D. J. Power, Decision Support, Analytics and Business Intelligence, Business Expert Press, 2019.
[21] D. J. Power and R. Sharda, Decision Support Systems, Springer, 2017.
[22] M. Negnevitsky, Artificial Intelligence: A Guide to Intelligent Systems, Pearson Education, 2011.
[23] F. Tao and Q. Qi, "Digital Twin Driven Smart Manufacturing," Journal of Manufacturing Systems, vol. 48, pp. 157–169, 2018.
[24] F. Tao, H. Zhang, A. Liu, and A. Nee, "Digital Twin in Industry: State-of-the-Art," IEEE Transactions on Industrial Informatics, vol. 15, no. 4, pp. 2405–2415, 2019.
[25] E. Fuller et al., "Digital Twin: Enabling Technologies, Challenges and Future Research," IEEE Access, vol. 8, pp. 108952–108971, 2020.
[26] J. Lee, B. Bagheri, and H. A. Kao, "A Cyber-Physical Systems Architecture for Industry 4.0-based Manufacturing Systems," Manufacturing Letters, vol. 3, pp. 18–23, 2015.
[27] X. Xu et al., "Industry 4.0 and Smart Manufacturing: A Review," International Journal of Production Research, vol. 59, no. 16, pp. 4967–4993, 2021.
[28] H. Boyes, B. Hallaq, J. Cunningham, and T. Watson, "The Industrial Internet of Things (IIoT): An Analysis Framework," Computers in Industry, vol. 101, pp. 1–12, 2018.
[29] M. Wooldridge, An Introduction to MultiAgent Systems, Wiley, 2020.
[30] T. Saaty, Decision Making with the Analytic Hierarchy Process, McGraw-Hill, 2008.
[31] P. Pedrycz and F. Gomide, Fuzzy Systems Engineering, Wiley, 2007.
[32] L. Breiman, "Random Forests," Machine Learning, vol. 45, no. 1, pp. 5–32, 2001.
[33] T. Chen and C. Guestrin, "XGBoost: A Scalable Tree Boosting System," Proceedings of KDD, pp. 785–794, 2016.
[34] C. Bishop, Pattern Recognition and Machine Learning, Springer, 2006.
[35] D. Silver et al., "Mastering the Game of Go with Deep Neural Networks and Tree Search," Nature, vol. 529, pp. 484–489, 2016.
[36] R. Khdhir et al., "Building Resilient National Critical Infrastructure: A Digital Twin-Based Framework for Comprehensive Insider and External Threat Detection," Journal of King Saud University – Computer and Information Sciences, 2026.
[37] F. Baiardi and V. Sammartino, "Simulation-Powered Cybersecurity: Real-Time Risk

IEER
Institute for Excellence in Education & Research

Assessment via Non-Intrusive Security Twin," The Journal of Supercomputing, 2026.
[38] P. Nguyen et al., "AI-Driven Digital Twin-Based Security Orchestration, Automation and Response for Critical Infrastructures," Automated Software Engineering, 2026.
[39] T. Gebhard and A. Tundis, "Distributed Resilience Assessment of Critical Infrastructures with Digital Twins Considering Uncertainty," Proceedings of IEEE DCOSS-IoT 2025, 2025.
[40] H. Marah et al., "TwinCompass: A Multi-Criteria and Hybrid Reasoning Decision Support Framework for Digital Twin Engineering in Cyber–Physical Systems," Journal of Industrial Information Integration, 2026.

IEER
Institute for Excellence in Education & Research