



TASK 2 – RESEARCH SKILLS 3

Chosen topic: Cybersecurity in a critical infrastructure of the energy sector

Field:
Cybersecurity

Prepared by

ALI MMADI, PhD student-Midocean University



Research Skills (3)

Task 2

ALI MMADI

PhD student - Midocean University

www.midocean.ae

INTRODUCTION

Hello everyone.

As part of Assignment 2 for the Research Skills 3 module, I will present an introduction to a scientific study in the field of Information Technology, specializing in cybersecurity, applied to critical infrastructures in the energy sector.

I will first present an introduction taken from a recognized thesis in the field of cybersecurity, explain the reasons for my choice, and offer some constructive critiques. Then, I will present my own research problem, adhering to the scientific criteria required for writing a solid academic introduction.



Presentation of the chosen introduction

The introduction I have chosen is taken from a thesis on the cybersecurity of critical energy infrastructures, in connection with the framework of the National Institute of Standards and Technology (NIST).

This introduction begins by presenting the overall context of the digital transformation of energy infrastructures. It explains how the digitization of power networks, especially SCADA systems and smart grids, has increased exposure to cyberattacks.

It then highlights:

- ☐ The global rise in cyber threats against critical infrastructures
- ☐ The economic and strategic risks
- ☐ The limitations of traditional cybersecurity approaches
- ☐ The need for a structured risk assessment framework

Why did I choose this introduction?

I chose it for three main reasons:

1. It follows the recommended pyramid structure: from general to specific.
2. It clearly justifies the importance of the topic with factual data.

It identifies a scientific gap in the assessment of protection strategies adapted to specific national contexts.

Constructive critique

However, according to my analysis:

- The introduction remains strongly oriented towards a North American context.
- It does not sufficiently develop the realities of developing countries.
- The research problem is introduced too late.

This shows that a good introduction must be contextualized and directly linked to the reality being studied.

Taking into account the methodological criteria studied in the course — notably clarity, scientific justification, the identification of a gap, and social relevance — I propose the following research question



RESEARCH PROBLEM

The digital transformation of critical infrastructure in the energy sector has significantly improved operational efficiency, remote monitoring, and automation of power grids. However, this increasing interconnection of industrial information systems has simultaneously expanded the attack surface against cyber threats.

Energy companies, especially in developing countries, face major challenges related to securing their SCADA systems, industrial networks, and strategic databases.

Despite the existence of international frameworks such as the NIST Cybersecurity Framework, their implementation often remains incomplete or ill-suited to local organizational, economic, and technical realities. Numerous studies have analyzed cyberattacks on critical infrastructures in industrialized countries, but few have focused on the actual assessment of the effectiveness of incident management strategies in institutional contexts where resources are limited.

Thus, the central issue of this research is as follows:

To what extent do current cybersecurity incident management strategies ensure the resilience of critical information systems in energy sector companies in developing countries?

This research will analyze two main variables:

- ☐ Independent variable: cybersecurity incident management strategies
- ☐ Dependent variable: level of resilience of critical information systems

The objective is to evaluate the effectiveness of existing mechanisms, identify structural weaknesses, and propose an improvement model adapted to the studied context.

This study aims to fill a scientific gap regarding the adaptation of international frameworks to local realities, while contributing to national security and the continuity of essential services.

Methodological points respected in my introduction

In writing this introduction and problem statement, I took into account the following essential elements:

- ❖ Presentation of the general context
- ❖ Clear identification of the problem
- ❖ Highlighting of a scientific gap
- ❖ Justification of academic and social importance
- ❖ Definition of variables
- ❖ Orientation towards a measurable objective

These elements correspond to the methodological recommendations studied in the course regarding the writing of a solid scientific introduction.

Conclusion

In conclusion, an effective introduction is not limited to presenting a topic, but it demonstrates the relevance, necessity, and originality of the research.

In the strategic field of critical infrastructure cybersecurity, methodological rigor is essential in order to produce actionable and scientifically valid results.

Thank you for your attention.

Documentation of the analyzed theses

- 1) Johnson, A. (2019).
Cybersecurity Risk Management in Critical Energy Infrastructure.
Doctoral Thesis, Massachusetts Institute of Technology (MIT), USA.
- 2) Alshamrani, A. (2020).
Evaluation of Incident Response Strategies in Industrial Control Systems.
PhD Dissertation, University of Manchester, United Kingdom.
- 3) Kim, H. (2018).
Resilience Assessment Models for Smart Grid Cybersecurity.
Doctoral Thesis, Seoul National University, South Korea.



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

