

Cybersecurity of Operators of Vital Importance

Prepared by

ALI MMADI, PhD student - Midocean University



Research Issues 1

Task 7

Zero Trust Architecture Implementation for Critical Infrastructure Protection: Lessons from National Power Grid Operators

Authors: Dubois, M. et al. (2024)

Journal: IEEE Transactions on Critical Infrastructure Protection

INTRODUCTION

In 2023, approximately 67% of critical infrastructure organizations experienced at least one significant cyber incident, and 23% faced multiple attacks. For this 7th task I analyze how the Zero Trust architecture protects vital operators such as electricity networks, relying on a case study conducted at RTE (Electricity Transport Network).



Title and variables

The title is clear:

- ☐ Independent: Zero Trust deployment level (micro-segmentation, MFA, etc.)
 - ☐ Dependent: Average time to detect intrusions (hours)
 - ☐ Moderator: Maturity of cyber governance processes
- The domain is crucial: an attack on an electrical grid can paralyze a country!

Central issue

The challenge: traditional network perimeters are ineffective against internal threats and APT.
Vital question: How to implement Zero Trust in aging industrial environments without disrupting critical operations?

Key best practices

The study reveals 3 imperatives:

- 1) **Granular micro-segmentation:** Isolation of SCADA/OT systems
 - 2) **Dynamic access:** MFA authentication + behavioral verification
 - 3) **Continuous telemetry:** 24/7 monitoring of network flows
- Result: 92% reduction in incidents at RTE in 18 months!

Conceptual model

- 1) Industrial sensors are isolated in secure areas
- 2) The dynamic access control validates each request
- 3) The SOC platform centralizes the logs and triggers responses

Equation:

$$\text{Confidence_score} = (\text{Identity_verification} \times \text{Risk_analysis})$$

Case study

Implementation at RTE:

- 1) 15,000 devices segmented into 78 secured zones
 - 2) Detection time reduced from 14 days to 43 minutes
 - 3) Cost: 0.8% of the annual IT budget, ROI in 9 months
- Proof:
Ransomware attack blocked in the initial phase!

Operational recommendations

The 5 golden rules:

- 1) Map ALL assets (including legacy systems)
- 2) Apply the principle of least privilege
- 3) Automate incident responses Train OT teams on cyber risks
- 4) Regularly audit third-party suppliers

CONCLUSION

Zero Trust is no longer an option for critical infrastructures. Next step: Integrate predictive AI. This research provides a reproducible framework for all vital sectors!

Key References

Main Article

1) Dubois, M. et al. (2024). *IEEE Transactions on Critical Infrastructure Protection*

↪ DOI: [10.1109/TCIP.2024.3389217](https://doi.org/10.1109/TCIP.2024.3389217)

2) Regulatory frameworks

NIS 2 Directive : ↪ eur-lex.europa.eu/NIS2

NIST Zero Trust Architecture : ↪ nist.gov/zero-trust

3) Real cases

RTE Cybersecurity Report 2024 : ↪ rte-france.com/cyber



مجموعة جامعة
الجميع الذكية
للتعليم القابضة

MIDOCEAN
UNIVERSITY



Thank You

