# 3. Protection of Critical Infrastructure Using an Integrated Cybersecurity Risk Management (i-CSRM) Framework

Kure, H. I., & Nwajana, A. O. (2022). Protection of critical infrastructure using an Integrated Cybersecurity Risk Management (i-CSRM) framework. In *Advances in computer and electrical engineering book series* (pp. 94–133). https://doi.org/10.4018/978-1-6684-3855-8.ch004

https://www.researchgate.net/publication/361116032_Protection_of_Critical_Infrastructure_Using_an_Integrated_Cybersecurity_Risk_Management_i-CSRM_Framework

1. **Role of Risk Management in Cyber-Physical Systems (CPS)**: The paper emphasizes the critical role of risk management in addressing cyber threats in CPS, focusing on the identification of critical assets, vulnerabilities, threats, and suitable proactive control measures for risk mitigation.
2. **Challenges Due to Complexity and Sophistication of Cyber Threats**: The increased complexity and sophistication of cyber-attacks in CPS environments make the task of risk management more challenging, as these threats are becoming less predictable.
3. **Objective of the Paper**: The aim is to enhance cybersecurity risk management (CSRM) practices by using asset criticality assessment, prediction of risk types, and evaluating the effectiveness of existing controls.
4. **Methodological Approach**: The paper proposes a unified approach that incorporates fuzzy set theory for asset criticality assessment, machine learning classifiers for risk prediction, and a comprehensive assessment model (CAM) for evaluating control effectiveness.
5. **Integration with CSRM Concepts and Data Sources**: The approach aligns with relevant CSRM concepts such as asset, threat actor, attack pattern, tactic, technique, and procedure (TTP), and utilizes the VERIS community dataset (VCDB) for risk prediction.
6. **Results and Effectiveness of the Approach**: Experimental results show that fuzzy set theory is effective in assessing asset criticality, and machine learning classifiers demonstrate strong performance in predicting various risk types, such as denial of service, cyber espionage, and crimeware.
7. **Contribution and Novelty of the Paper**: The paper's contributions are fourfold: using fuzzy logic for asset criticality assessment, employing various machine learning models for risk type prediction, adopting a comprehensive assessment model for control effectiveness,

and using VCDB for risk prediction. These contributions collectively enhance the overall risk management process in cybersecurity.