A Software Engineering Framework for Secure Cyber Risk Governance in Critical Energy Infrastructure: A PRISMA-Based Systematic Review

VFAST Transactions on Software Engineering • Article • *Open Access* • 2026 •
DOI: 10.21015/vtse.v14i2.2471

Rodzoan, Muhammad Asyraf Bin [a] ; Ahmed, Husham M. [b] ;
Jamaluddin, Mohammed Darwis Haikal Bin [c] ; Koondhar, Muhammad Yaqoob [d]

[a] Kulliyyah Information & Communication Technology, International Islamic University, IIUM, Gombak, Malaysia

Abstract

The digitalization of critical energy infrastructure has turned cybersecurity from an IT-related problem into a more generalized software engineering and risk governance issue. Previous research has focused on studying cyber threats, regulatory needs, and operational resilience individually, but little work has been done to combine secure software engineering practices and cyber risk governance in the energy sector. This study aims to fill this gap by conducting a systematic literature review in line with PRISMA 2020. A total of 1,092 records were identified, of which 70 studies were finally included. The review draws evidence from various sources to provide a synthesis of the issues surrounding IT/OT convergence, ransomware, supply-chain vulnerabilities, artificial intelligence,

and new regulations on critical energy systems cybersecurity. The results show that cyber resilience is not about compliance, as it is a life-long process of software development rather than an end-of-pipe security objective. From the literature review, a four-pillar approach involving regulatory compliance, operational technology security, third-party risk management, and AI governance is suggested and connected to SS-DLC and DevSecOps principles. It encourages a continuous lifecycle security exercise, architectures that are designed with security in mind, and the continuous validation of security for critical infrastructure applications. This study provides a unified software engineering perspective that links cyber risk governance with practices of software development. The proposed framework offers actionable steps to help software engineers, cybersecurity professionals, and policymakers enhance resilience, boost readiness for compliance, and aid in the secure advancement and modernization of critical energy infrastructure.

Author keywords

Artificial Intelligence Governance; Critical Infrastructure Security; Cyber Risk Governance; DevSecOps; OT Security; PRISMA Systematic Review; Secure Software Development; Software Engineering; SSDLC

Funding details

Details about financial support for research, including funding sources and grant numbers as provided in academic publications.

Funding sponsor	Funding number	Acronym
International Islamic University Malaysia See opportunities by IIUM		IIUM
Tenaga Nasional Berhad See opportunities by TNB		TNB
Group Legal Department		
University of Technology Bahrain		
Kulliyyah of Information and Communication Technology		

Funding text

The authors gratefully acknowledge the institutional support of the Kulliyyah of Information and Communication Technology, International Islamic University Malaysia (IIUM), the College of Engineering, University of Technology Bahrain, and the Group Legal Department, Tenaga Nasional Berhad (views expressed in a personal academic capacity of the author, not on behalf of Tenaga Nasional Berhad).

Corresponding authors

Corresponding author	M.A.B. Rodzoan
Affiliation	Kulliyyah Information & Communication Technology, International Islamic University, IIUM, Gombak, Malaysia
Email address	asyrafrodzoan@iium.edu.my

About Scopus

Language

查看繁體中文版本

Просмотр версии на русском языке

Customer Service

Help

Tutorials

Contact us

ELSEVIER