ABSTRACT

This research analyzes information security risks arising from the integration of Information Technology (IT) and Operational Technology (OT) in a power generation system at PT PLN Nusantara Power UP Muara Karang. The digitalization of industrial control systems has created an integrated environment known as IT/OT convergence, which connects commonly used OT components in power plants with the iCORE analytics platform.

Previous studies on industrial control system security and IT/OT convergence have generally focused on network architecture or compliance with security standards, while limited attention has been given to process data as a critical information asset that directly supports analytics and operational decision-making. Therefore, this study focuses on assessing information security risks related to OT process data flowing through the IT/OT convergence system and utilized by iCORE.

The OCTAVE Allegro method is employed due to its asset-based risk assessment approach that considers operational impacts, making it suitable for analyzing information security risks in IT/OT convergence environments within power plants. The risk assessment process includes identifying critical information assets, mapping relevant threats and vulnerabilities, and determining risk levels based on applicable threat scenarios.

The results identify five main threat scenarios, three of which fall into the high-priority risk category. These threats include malware infection via removable media, misuse of administrative access privileges, and potential intrusion from the IT network to the OT domain due to insufficient network segmentation. The findings provide an overview of the information security risk conditions in the IT/OT convergence system and serve as a basis for formulating relevant risk mitigation recommendations for information security management in power generation environments.

Keywords : *information security, IT/OT convergence, OCTAVE Allegro, cybersecurity risk*

INTISARI

Penelitian ini menganalisis risiko keamanan informasi yang muncul akibat integrasi antara Information Technology (IT) dan Operational Technology (OT) pada sistem pembangkit listrik di PT PLN Nusantara Power UP Muara Karang. Digitalisasi sistem kendali industri telah menciptakan lingkungan terintegrasi yang dikenal sebagai sistem konvergensi IT/OT, yang menghubungkan komponen OT yang lazim digunakan pada pembangkit listrik dengan platform analitik iCORE.

Penelitian-penelitian sebelumnya mengenai keamanan sistem kendali industri dan konvergensi IT/OT umumnya berfokus pada aspek teknis arsitektur jaringan atau kepatuhan terhadap standar keamanan, namun masih terbatas dalam menganalisis data proses OT sebagai aset informasi kritis yang berperan langsung dalam analitik dan pengambilan keputusan operasional. Oleh karena itu, penelitian ini difokuskan pada analisis risiko keamanan informasi terhadap data proses OT yang mengalir melalui sistem konvergensi IT/OT dan dimanfaatkan oleh iCORE.

Metode OCTAVE Allegro digunakan dalam penelitian ini karena pendekatannya berfokus pada penilaian risiko berbasis aset dengan mempertimbangkan dampak operasional, sehingga sesuai untuk menganalisis risiko keamanan informasi pada lingkungan konvergensi IT/OT di pembangkit listrik. Proses penilaian risiko dilakukan melalui identifikasi aset informasi kritis, pemetaan ancaman dan kerentanan, serta penentuan tingkat risiko berdasarkan skenario ancaman yang relevan.

Hasil penelitian mengidentifikasi lima skenario ancaman utama, dengan tiga di antaranya berada pada kategori risiko prioritas tinggi. Ancaman tersebut meliputi infeksi malware melalui removable media, penyalahgunaan hak akses administratif, serta potensi intrusi dari jaringan IT ke OT akibat segmentasi jaringan yang belum optimal. Temuan ini memberikan gambaran mengenai kondisi risiko keamanan informasi pada sistem konvergensi IT/OT dan menjadi dasar penyusunan rekomendasi mitigasi yang relevan bagi pengelolaan keamanan informasi di lingkungan pembangkit listrik.

Kata kunci – keamanan informasi, konvergensi IT/OT , OCTAVE Allegro, risiko keamanan siber