ANALISIS KERENTANAN STRATEGI KONTROL PADA REAKTOR PROSES VINIL ASETAT TERHADAP SERANGAN SIBER

Putri Alya Wulandari

21/473347/TK/52161

Diajukan kepada Departemen Teknik Nuklir dan Teknik Fisika Fakultas Teknik
Universitas Gadjah Mada pada tanggal 21 April 2025
untuk memenuhi sebagian persyaratan untuk memperoleh derajat
Sarjana Program Studi Teknik Fisika

INTISARI

Industrial Control System (ICS), seperti SCADA, DCS, dan PLC, yang mulanya terisolasi kini terintegrasi dengan jaringan digital melalui *Industrial Internet of Things* (IIoT). Hal ini meningkatkan risiko serangan siber fisik yang mengancam keselamatan dan operasional industri. Unit reaktor, sebagai inti dari proses produksi, rentan terhadap serangan siber karena kompleksitas dan ketergantungannya terhadap integritas data kontrol. Serangan siber dapat memanipulasi data atau mengganggu komunikasi dalam sistem, yang dapat menyebabkan kegagalan fungsi sistem. Oleh karena itu, diperlukan analisis kerentanan strategi kontrol reaktor terhadap serangan siber.

Penelitian ini melibatkan simulasi proses vinil asetat menggunakan strategi kontrol pengendalian umpan balik dan rasio untuk mengatur umpan reaktor. Kedua strategi kontrol tersebut akan dianalisis kerentanannya terhadap serangan *Denial of Service* (DoS) dan integritas. Analisis kerentanan ditinjau dari dampak serangan siber terhadap perubahan laju aliran, komposisi, dan kerugian ekonomi.

Hasil penelitian menunjukkan bahwa pengendalian rasio lebih rentan terhadap serangan DoS dan integritas dibandingkan pengendalian umpan balik. Pada serangan DoS, pengendalian rasio menyebabkan kerugian ekonomi dan kehilangan produksi 13% lebih besar dari pengendalian umpan. Pada serangan integritas, pengendalian rasio juga menimbulkan kerugian ekonomi dan kehilangan produksi yang lebih besar, yaitu 17,45% lebih tinggi dibandingkan pengendalian umpan balik. Meskipun demikian, kedua strategi kontrol mampu mempertahankan kualitas produk mendekati 0,95 mol% ketika terjadi serangan siber.

Kata kunci: *Denial of Service*, *industrial internet of things*, integritas, kerentanan, strategi kontrol

Pembimbing Utama : Dr.-Ing. Ir. Awang N. I. W., S.T., M.Sc., IPM.

Pembimbing Pendamping : Dr.-Ing. Sihana

VULNERABILITY ANALYSIS OF CONTROL STRATEGIES IN VINYL ACETATE PROCESS REACTORS AGAINST CYBER ATTACKS

Putri Alya Wulandari

21/473347/TK/52161

Submitted to the Department of Nuclear Engineering and Engineering Physics
Faculty of Engineering Universitas Gadjah Mada on April 21, 2025
in partial fulfillment of the requirement for the Degree of
Bachelor of Engineering in Engineering Physics

ABSTRACT

Industrial Control Systems (ICS), such as SCADA, DCS, and PLCs, which were initially isolated, are now integrated with the digital network through the Industrial Internet of Things (IIoT). This integration increases the risk of cyber-physical attacks that threaten industrial safety and operations. The reactor unit, as the core of the production process, is vulnerable to cyber attacks due to its complexity and reliance on the integrity of control data. Cyber attacks can manipulate data or disrupt communication within the system, potentially causing system failures. Therefore, it is essential to analyze the vulnerability of reactor control strategies to cyber attacks.

This study involves a simulation of the vinyl acetate process using feedback and ratio control strategies to control the reactor feed. The vulnerability of both control strategies is analyzed under Denial of Service (DoS) and integrity attacks. The vulnerability analysis focuses on the impact of cyber attacks on flow rate changes, composition, and economic losses.

The results show that ratio control is more vulnerable to both DoS and integrity attacks compared to feedback control. Under DoS attacks, ratio control results in 13% higher economic losses and production losses than feedback control. In integrity attacks, ratio control also causes greater losses, 17.45% higher than feedback control. Nevertheless, both control strategies were able to maintain product quality close to 0.95 mol% during the cyber attacks.

Keywords: control strategies, Denial of Service, industrial internet of things, integrity, vulnerability

Supervisor : Dr.-Ing. Ir. Awang N. I. W., S.T., M.Sc., IPM.

Co-supervisor : Dr.-Ing. Sihana