https://ejournal.polsub.ac.id/index.php/j-mame
Jurusan Teknik Mesin
Politeknik Negeri Subang

J-MAME
Journal of Maintenance and Mechanical Engineerint

PENERAPAN KESELAMATAN DAN KESEHATAN KERJA PADA SISTEM OTOMASI BERBASIS PLC: KAJIAN RISIKO, HUMAN ERROR, DAN KEAMANAN SISTEM

Fahmi Maulana [1)*], Oktoria Simanjuntak[2)], Prasetyo Dwi N[3)], Refalah Al Falaknaz[4)], Dino Dwi Aryanto[5)]

[1,2,3,4,5)]Program Studi Teknik Mesin, Jurusan Teknik Mesin, Politeknik Negeri Subang. Blok Kaleng Banteng Desa Cibogo, Kec. Cibogo, Kabupaten Subang, Jawa Barat 41285, Indonesia
[*]email korespondensi: oktoriasimanjuntak9@gmail.com

INFORMASI ARTIKEL

Received:
16/10/26

Received in revised:
17/11/26

Accepted:
18/11/26

Online-Published:
22/11/26

ABSTRAK

Programmable Logic Control (PLC) dan sistem kendali banyak digunakan dalam pelaksanaan praktikum otomasi untuk menghubungkan pemograman, rangkaian listrik, sensor, aktuator dan proses kerja mesin. Meskipun PLC dapat meningakatkan keteraturan dan otomasi proses, namun kegiatan praktikum tetap memiliki potensi bahaya berupa sengatan listrik, gerakan aktuator yang tidak terduga, kesalahan pengawatan, kesalahan program, serta pengoprasian tanpa prosedur keselamatan. Artikel ini juga bertujuan untuk meninjau penerapan keselamatan dan kesehatan kerja (K3) pada pengunaan PLC pada sistem kendali, mengidentifikasi bentuk kesalahan yang berpotensi terjadi selama melaksanakan praktikum, serta merumuskan pengendalian yang dapat diterapkan. Metode yang digunakan adalah studi literatur dengan menelaah penelitian tentang penilaian risiko pada otomasi berbasis PLC, HIRARC pada lingkungan kerja, serta prinsip keselamatan mesin dan sistem kendali. Hasil kajian menunjukkan bahwa pengendalian yang efektif perlu menggabungkan identifikasi bahaya sebelum praktikum, pemeriksaan kondisi panel dan kabel, SOP, pengamanan sumber energi, verifikasi program sebelum dijalankan, penggunan APD yang sesuai, tombol penghentian darurat, dan pengawasan. Penerapan pendekatan hirarki pengendalian serta penilaian risiko berbasis HIRARC/ISO 12100 dapat menjadi dasar perbaikan K3 pada praktikum PLC dan sistem kendali.

***Kata Kunci** : K3, PLC, Sistem Kendali, HIRARC, ISO 12100*

ABSTRACT

Programmable Logic Controllers (PLCs) and control systems are widely used in automation practical sessions to integrate programming, electrical circuits, sensors, actuators, and machine operation processes. Although PLCs can improve process organization and automation, practical activities still involve potential hazards such as electric shock, unexpected actuator movements, wiring errors, programming errors, and

operation without proper safety procedures. This article aims to review the implementation of occupational safety and health (OSH) in the use of PLCs in control systems, identify potential errors that may occur during practical sessions, and formulate applicable control measures. The method used is a literature review by examining studies on risk assessment in PLC-based automation, HIRARC in the workplace, and the principles of machine and control system safety. The results indicate that effective control measures should integrate hazard identification before practical sessions, inspection of panels and cables, standard operating procedures (SOPs), energy source isolation, program verification before execution, the use of appropriate personal protective equipment (PPE), emergency stop buttons, and supervision. The application of the hierarchy of controls approach and risk assessment based on HIRARC/ISO 12100 can serve as a basis for improving occupational safety and health in PLC and control system practical sessions.

Keywords : ***OSH, Control System, HIRARC, ISO 12100***

1. PENDAHULUAN

Perkembangan teknologi otomasi industri telah meningkatkan penggunaan *Programmable Logic Controller* (PLC) sebagai salah satu komponen utama dalam sistem kendali industri atau *Industrial Control System* (ICS). PLC berfungsi menerima masukan dari *push button*, sensor, dan perangkat input lainnya, kemudian memprosesnya berdasarkan program yang telah dibuat untuk menghasilkan keluaran berupa pengendalian lampu indikator, relay, motor, solenoid, maupun aktuator. Penerapan PLC tidak hanya ditemukan pada lingkungan industri, tetapi juga dalam kegiatan pendidikan vokasi sebagai sarana pembelajaran yang menghubungkan pemrograman, rangkaian listrik, sistem kendali, sensor, aktuator, dan proses kerja mesin secara langsung.

ICS banyak digunakan untuk mengendalikan dan memantau infrastruktur penting, seperti pembangkit listrik, sistem transportasi, pengolahan air, serta berbagai proses produksi di industri. Sistem tersebut termasuk dalam lingkungan *Operational Technology* (OT) yang memiliki karakteristik berbeda dengan *Information Technology* (IT), terutama karena menuntut tingkat ketersediaan yang tinggi (*high availability*) dan kemampuan operasi secara *real-time*. Kondisi tersebut menyebabkan penerapan sistem keamanan dan pengendalian risiko pada ICS perlu dilakukan secara tepat agar tidak mengganggu proses operasi. Seiring dengan meningkatnya konektivitas jaringan dan penggunaan teknologi berbasis internet, ICS juga semakin menghadapi ancaman keamanan siber. Beberapa serangan yang pernah terjadi pada sistem industri antara lain Stuxnet, TRITON, BlackEnergy, dan Havex. Serangan terhadap PLC dapat dilakukan melalui penyisipan, perubahan, atau manipulasi program secara tidak sah sehingga berpotensi memengaruhi proses pengendalian sistem.

Ancaman pada sistem berbasis PLC tidak hanya berkaitan dengan keamanan informasi, tetapi juga dapat berdampak terhadap keselamatan manusia dan peralatan. Manipulasi program atau kesalahan pengendalian dapat menyebabkan aktuator bekerja di luar kondisi yang diharapkan, sehingga meningkatkan kemungkinan terjadinya kecelakaan maupun kerusakan peralatan. Oleh karena itu, aspek keselamatan dalam penggunaan PLC perlu diperhatikan secara menyeluruh, baik dari sisi perangkat keras, program, pengawatan, prosedur kerja, maupun perilaku pengguna. Penelitian mengenai *Mechanical Hazard Simulator of PLC-Based Automation Technology According to ISO 12100* menunjukkan bahwa sistem otomasi berbasis PLC perlu melalui proses identifikasi dan

penilaian risiko sebelum diterapkan karena mesin otomasi dapat memiliki berbagai kondisi berbahaya yang berpotensi mengancam keselamatan. Pendekatan berbasis ISO 12100 dan tindakan *retrofit* dapat digunakan untuk mengurangi tingkat risiko pada sistem otomasi (’Adil et al., 2025).

Dalam kegiatan praktikum PLC, potensi bahaya tidak hanya berasal dari sistem otomasi dan perangkat yang digunakan, tetapi juga dapat muncul akibat kesalahan manusia (*human error*) dan kondisi instalasi yang kurang aman. Beberapa kondisi yang berpotensi menimbulkan kecelakaan antara lain melakukan pengawatan saat sumber listrik masih aktif, kesalahan pemasangan kabel atau terminal, kabel yang tidak memiliki identitas, terminal yang longgar, menjalankan program yang belum diverifikasi, serta berada terlalu dekat dengan bagian mesin yang bergerak ketika sistem diaktifkan. Selain itu, kurangnya pemeriksaan rangkaian sebelum pemberian sumber listrik dan ketidaksesuaian prosedur kerja dapat meningkatkan risiko sengatan listrik, hubungan pendek, kerusakan komponen, maupun gerakan aktuator yang tidak terduga.

Penerapan keselamatan dan kesehatan kerja (K3) menjadi salah satu upaya penting untuk mengendalikan berbagai risiko tersebut. Identifikasi bahaya dan penilaian risiko dapat dilakukan menggunakan metode HIRARC (*Hazard Identification, Risk Assessment and Risk Control*), yaitu pendekatan yang digunakan untuk mengenali sumber bahaya, menentukan tingkat risiko, serta menetapkan tindakan pengendalian yang sesuai. Penerapan HIRARC pada lingkungan laboratorium dapat dilakukan melalui penyediaan fasilitas keselamatan, pengaturan tata letak peralatan, pemberian pelatihan, penggunaan alat pelindung diri (APD), serta penerapan prosedur operasi standar (SOP) (Mahendra et al., 2025). Pada lingkungan ketenagalistrikan, metode HIRARC juga dapat digunakan untuk mengidentifikasi berbagai risiko, seperti sengatan listrik dan kebakaran, sekaligus menentukan langkah pengendalian yang sesuai (Widana et al., 2024).

Selain aspek keselamatan fisik, keamanan program PLC juga perlu menjadi perhatian dalam penerapan sistem kendali. Pemantauan terhadap perubahan program dapat dilakukan untuk mendeteksi adanya penyisipan atau manipulasi program yang tidak sah. Salah satu pendekatan yang dapat digunakan adalah sistem pemantauan blok program PLC yang terdiri atas modul akuisisi memori untuk mengambil data dari memori PLC, modul pemantauan untuk membandingkan data dan mendeteksi perubahan, serta modul pencatatan (*logging*) untuk merekam perubahan dan memberikan alarm ketika teridentifikasi adanya manipulasi. Sistem tersebut perlu dirancang dengan mempertimbangkan karakteristik operasi PLC yang membutuhkan respons secara *real-time*, sehingga mekanisme keamanan tidak menyebabkan gangguan terhadap proses kendali.

Berdasarkan uraian tersebut, penerapan K3 pada praktikum PLC dan sistem kendali perlu mencakup pengendalian terhadap bahaya listrik, mekanis, kesalahan pengawatan, kesalahan program, faktor manusia, serta ancaman keamanan terhadap program PLC. Pendekatan keselamatan yang terintegrasi diperlukan agar sistem dapat digunakan secara aman tanpa mengurangi fungsi dan kinerja proses kendali. Oleh karena itu, artikel ini bertujuan untuk meninjau penerapan K3 pada kegiatan praktikum PLC dan sistem kendali, mengidentifikasi berbagai kesalahan dan kondisi tidak aman yang berpotensi terjadi, serta merumuskan rekomendasi pengendalian risiko yang dapat diterapkan untuk menciptakan kegiatan praktikum yang aman, teratur, dan sesuai dengan prinsip keselamatan kerja.

2. METODE

Penelitian ini menggunakan metode studi literatur dengan pendekatan deskriptif. Sumber yang dikaji terdiri atas artikel jurnal yang membahas keselamatan pada otomasi berbasis PLC, penilaian risiko HIRARC, keselamatan mesin berdasarkan ISO 12100, serta prinsip keselamatan sistem kendali. Template J-MAME digunakan sebagai dasar penyusunan struktur artikel, sedangkan sumber ilmiah digunakan untuk membangun pembahasan dan rekomendasi.

2.1. Tahapan Kajian

Tahapan kajian meliputi pencarian literatur, seleksi sumber yang relevan, pengelompokan informasi, identifikasi bahaya, analisis kesalahan pelaksanaan, dan penyusunan rekomendasi pengendalian. Literatur utama yang digunakan adalah penelitian ’Adil et al. (2025) mengenai penilaian risiko otomasi berbasis PLC menurut ISO 12100,

penelitian Mahendra et al. (2025) mengenai HIRARC pada laboratorium, penelitian Widana et al. (2024) mengenai HIRARC pada instalasi kelistrikan, serta penelitian mengenai prosedur dan pengetahuan K3 terhadap kecelakaan kerja (Imasya Putri et al., 2021).

2.2.Analisis Risiko

Analisis risiko dilakukan dengan menghubungkan aktivitas praktikum dengan sumber bahaya, dampak yang mungkin terjadi, dan tindakan pengendalian. Prinsip ISO 12100 menekankan identifikasi bahaya dan pengurangan risiko melalui langkah pengendalian yang sistematis. Dalam praktik laboratorium, pendekatan tersebut dapat diterapkan secara sederhana melalui urutan: identifikasi bahaya, penilaian kemungkinan dan keparahan, penentuan tingkat risiko, pemilihan pengendalian, dan pemeriksaan kembali setelah pengendalian diterapkan.

2.3.Objek yang Ditinjau

Objek tinjauan meliputi panel/trainer PLC, power supply, push button, sensor, relay, lampu indikator, aktuator, kabel pengawatan, perangkat pemrograman, serta proses pengujian program. Fokus keselamatan diarahkan pada interaksi manusia dengan sumber listrik dan gerakan mekanis, kesalahan pengawatan, kesalahan logika program, serta prosedur saat melakukan perubahan atau pemeriksaan rangkaian.

3. HASIL DAN PEMBAHASAN

Keamanan sistem merupakan salah satu aspek penting dalam penerapan Keselamatan dan Kesehatan Kerja (K3) pada industri yang menggunakan teknologi otomasi berbasis Programmable Logic Controller (PLC). PLC berfungsi sebagai perangkat pengendali yang mengatur proses kerja mesin melalui program logika, pembacaan sinyal sensor, serta pengiriman perintah kepada aktuator. Dalam penerapannya, PLC tidak hanya bekerja secara mandiri, tetapi juga dapat terhubung dengan perangkat lain, seperti Human Machine Interface (HMI), Supervisory Control and Data Acquisition (SCADA), sensor digital, jaringan komunikasi industri, dan komputer pengawas. Keterhubungan tersebut memberikan kemudahan dalam pemantauan serta pengendalian proses produksi, tetapi juga menimbulkan potensi kerentanan terhadap gangguan keamanan sistem. Ancaman tersebut dapat berupa akses tidak sah, perubahan program PLC, pencurian data, penyisipan instruksi berbahaya, hingga gangguan komunikasi antara perangkat kontrol. Oleh karena itu, keamanan sistem perlu diterapkan sebagai bagian dari upaya pencegahan kecelakaan kerja dan perlindungan terhadap keandalan proses produksi.

Dalam lingkungan industri, keamanan sistem otomasi dikenal dengan istilah *Operational Technology Security* (OT Security), yaitu perlindungan terhadap perangkat keras, perangkat lunak, dan jaringan yang digunakan untuk memantau serta mengendalikan proses fisik. Berbeda dengan keamanan teknologi informasi (*Information Technology Security* atau IT Security) yang umumnya berfokus pada kerahasiaan, integritas, dan ketersediaan informasi, keamanan OT juga harus mempertimbangkan keselamatan manusia, keandalan mesin, dan keberlangsungan proses produksi. Sebagai contoh, perubahan tidak sah terhadap program PLC pada mesin press hidrolik dapat menyebabkan aktuator bergerak tanpa perintah yang sesuai sehingga berpotensi menjepit atau mencederai operator. Dengan demikian, gangguan keamanan pada sistem otomasi tidak hanya menimbulkan kerugian berupa kehilangan data atau berhentinya produksi, tetapi juga dapat berkembang menjadi bahaya fisik yang mengancam keselamatan pekerja.

3.1. Jenis Ancaman Keamanan pada Sistem PLC

Sistem otomasi berbasis PLC memiliki beberapa jenis ancaman keamanan yang perlu diperhatikan karena setiap ancaman dapat memengaruhi proses pengendalian mesin. Ancaman tersebut dapat berasal dari faktor internal maupun eksternal. Faktor internal dapat berupa kelalaian operator, teknisi, atau administrator yang memiliki akses terhadap sistem, sedangkan faktor eksternal dapat berasal dari pihak yang mencoba masuk ke jaringan industri tanpa izin. Beberapa bentuk ancaman keamanan pada sistem PLC dijelaskan sebagai berikut.

a) **Akses Tidak Sah (*Unauthorized Access*)**

Akses tidak sah merupakan kondisi ketika seseorang memperoleh akses terhadap PLC, HMI, komputer pemrograman, atau jaringan industri tanpa izin dan kewenangan yang sesuai. Kondisi ini dapat terjadi akibat penggunaan kata sandi yang lemah, penggunaan akun bersama, tidak adanya pembatasan hak akses, atau tidak adanya sistem autentikasi yang memadai. Apabila pihak yang tidak berwenang berhasil mengakses PLC, pihak tersebut dapat melihat, mengubah, bahkan menghapus program pengendalian mesin. Sebagai contoh, seseorang yang memperoleh akses ke PLC mesin CNC dapat mengubah parameter gerakan sumbu atau urutan kerja mesin sehingga pergerakan mesin tidak lagi sesuai dengan prosedur operasional. Hal tersebut dapat menyebabkan kerusakan benda kerja, kerusakan komponen mesin, dan meningkatkan risiko kecelakaan bagi operator. Oleh karena itu, setiap pengguna harus memiliki akun dan hak akses sesuai dengan tanggung jawab pekerjaannya.

b) **Manipulasi Program PLC (*PLC Program Manipulation*)**

Manipulasi program PLC merupakan tindakan mengubah instruksi atau logika pengendalian yang telah dibuat tanpa prosedur pemeriksaan dan persetujuan yang benar. Perubahan tersebut dapat dilakukan secara sengaja oleh pihak yang tidak bertanggung jawab maupun secara tidak sengaja oleh teknisi yang melakukan kesalahan saat pemrograman. Program PLC yang telah dimanipulasi dapat menyebabkan sensor tidak terbaca dengan benar, sistem interlock tidak bekerja, atau aktuator menerima perintah yang tidak sesuai dengan kondisi sebenarnya. Contohnya, pada mesin press hidrolik, program yang seharusnya menghentikan gerakan ram ketika pelindung pengaman terbuka dapat diubah sehingga mesin tetap beroperasi meskipun operator berada di area berbahaya. Kondisi ini menunjukkan bahwa integritas program PLC memiliki hubungan langsung dengan keselamatan kerja. Upaya pencegahannya dapat dilakukan melalui pembatasan akses pemrograman, pencatatan perubahan program, pemeriksaan logika sebelum mesin dioperasikan, serta penyimpanan salinan program yang telah diverifikasi.

c) **Serangan Malware dan Perangkat Lunak Berbahaya**

Malware merupakan perangkat lunak berbahaya yang dapat digunakan untuk mengganggu, merusak, atau mengambil alih fungsi suatu sistem komputer. Dalam lingkungan industri, malware dapat masuk melalui komputer pemrograman PLC, perangkat penyimpanan eksternal, jaringan perusahaan, maupun koneksi jarak jauh yang tidak terlindungi. Salah satu contoh ancaman yang pernah terjadi adalah Stuxnet, yaitu malware yang dirancang untuk menyerang sistem kontrol industri dan memanipulasi operasi perangkat tertentu. Keberadaan malware pada lingkungan otomasi dapat menyebabkan perubahan instruksi kontrol, gangguan komunikasi, ketidakakuratan pemantauan, hingga penghentian proses produksi. Apabila malware memengaruhi sistem pengendalian keselamatan, dampaknya dapat berupa pergerakan mesin yang tidak terkendali atau kegagalan fungsi perlindungan. Oleh sebab itu, komputer pemrograman dan jaringan industri harus dilindungi melalui pengendalian perangkat eksternal, pemeriksaan keamanan, pembaruan sistem yang terencana, serta pembatasan koneksi terhadap jaringan yang tidak diperlukan.

d) **Gangguan Komunikasi Jaringan (*Network Attack*)**

Gangguan komunikasi jaringan merupakan ancaman yang terjadi ketika komunikasi antara PLC, HMI, SCADA, sensor, atau perangkat pengendali lainnya mengalami gangguan akibat aktivitas yang tidak sah. Bentuk gangguan dapat berupa penyadapan komunikasi, pemalsuan pesan, manipulasi data, maupun serangan yang menyebabkan perangkat

kehilangan koneksi. Kondisi tersebut dapat membuat operator menerima informasi yang tidak sesuai dengan keadaan mesin sebenarnya. Sebagai contoh, apabila data sensor tekanan pada sistem hidrolik dimanipulasi, HMI dapat menampilkan nilai tekanan yang berbeda dari tekanan aktual sehingga operator salah mengambil keputusan. Gangguan komunikasi juga dapat menyebabkan perintah kendali terlambat diterima atau tidak diteruskan kepada aktuator. Dalam sistem otomasi yang membutuhkan respons cepat, kondisi tersebut berpotensi mengganggu kestabilan proses dan meningkatkan risiko kecelakaan. Pencegahannya dapat dilakukan melalui segmentasi jaringan, pengamanan protokol komunikasi, pemantauan lalu lintas jaringan, dan pembatasan koneksi antarsistem.

e) **Penyalahgunaan Hak Akses oleh Pengguna Internal (*Insider Threat*)**

Ancaman keamanan tidak selalu berasal dari pihak luar, tetapi juga dapat terjadi akibat tindakan pengguna internal yang memiliki akses terhadap sistem. Operator, teknisi, maupun administrator dapat menimbulkan risiko apabila menggunakan kewenangannya tanpa mengikuti prosedur keamanan yang telah ditetapkan. Contohnya adalah penggunaan akun teknisi oleh beberapa orang, penonaktifan sensor pengaman tanpa izin, pengubahan program PLC tanpa dokumentasi, serta penggunaan mode manual untuk melewati sistem interlock. Tindakan tersebut dapat menyebabkan sistem kehilangan fungsi perlindungan yang seharusnya mencegah mesin bekerja dalam kondisi berbahaya. Ancaman internal juga berkaitan erat dengan faktor *human error*, karena kurangnya pemahaman dan kedisiplinan pekerja dapat membuka peluang terjadinya gangguan keamanan. Oleh karena itu, pengendalian keamanan perlu disertai pelatihan, pembagian tanggung jawab, pengawasan, dan penerapan prosedur kerja yang jelas.

f) **Kegagalan Sistem Pengamanan (*Security Control Failure*)**

Kegagalan sistem pengamanan terjadi ketika mekanisme perlindungan yang seharusnya menjaga keamanan dan keselamatan sistem tidak berfungsi sebagaimana mestinya. Kondisi ini dapat disebabkan oleh konfigurasi yang tidak tepat, perangkat pengaman yang dinonaktifkan, sensor yang mengalami kerusakan, atau tidak dilakukannya pemeriksaan secara berkala. Pada sistem otomasi, kegagalan tersebut dapat menyebabkan mesin tetap beroperasi meskipun terdapat kondisi yang seharusnya menghentikan proses kerja. Sebagai contoh, sistem interlock pada mesin frais seharusnya mencegah mesin beroperasi ketika pelindung mesin terbuka. Namun, apabila fungsi interlock dinonaktifkan atau program PLC diubah tanpa pemeriksaan, mesin dapat tetap bekerja dan membahayakan operator. Oleh karena itu, sistem pengamanan harus diperiksa secara berkala melalui pengujian fungsi, pemeriksaan konfigurasi, dan evaluasi terhadap seluruh perangkat keselamatan.

3.2. Dampak Ancaman Keamanan Sistem terhadap Keselamatan dan Kesehatan Kerja

Ancaman keamanan pada sistem otomasi berbasis PLC dapat berdampak langsung maupun tidak langsung terhadap penerapan K3 di lingkungan industri, karena sistem digital terhubung erat dengan proses fisik mesin. Ketika sistem kontrol terganggu, mesin dapat menerima perintah yang salah, kehilangan fungsi pengamanan, atau tidak merespons sesuai kondisi operasional sebenarnya.

a) Dampak pertama adalah meningkatnya risiko kecelakaan kerja akibat pergerakan mesin yang tidak terkendali. Manipulasi program atau gangguan sensor dapat menggerakkan aktuator saat operator melakukan pemeriksaan atau perawatan, sehingga pekerja berisiko terjepit, tertimpa, tersayat, atau terbentur komponen mesin.
b) Dampak kedua adalah kegagalan fungsi perangkat keselamatan. Emergency stop, safety interlock, light curtain, dan sensor pengaman berfungsi menghentikan mesin saat kondisi berbahaya terdeteksi. Jika perangkat tersebut terganggu, dinonaktifkan, atau tidak terintegrasi dengan benar, perlindungan terhadap pekerja menurun. Pada mesin press hidrolik, misalnya, kegagalan komunikasi antara sensor pengaman dan

sistem kontrol dapat membuat mesin tetap bergerak meskipun ada objek atau anggota tubuh manusia di area kerja.

c) Dampak ketiga adalah kesalahan pengambilan keputusan oleh operator. Gangguan keamanan dapat membuat informasi pada HMI tidak sesuai dengan kondisi aktual, sehingga operator salah menafsirkan tekanan, temperatur, posisi aktuator, atau status mesin dan mengambil tindakan yang keliru.

d) Dampak keempat adalah terganggunya keandalan dan keberlangsungan produksi. Serangan pada jaringan industri atau kerusakan program PLC dapat menghentikan mesin secara mendadak, menunda produksi, dan merusak komponen. Dalam kondisi tertentu, gangguan ini juga dapat menimbulkan kebocoran fluida, peningkatan tekanan, atau pelepasan energi yang tidak terkendali. Dengan demikian, keamanan sistem tidak hanya berkaitan dengan perlindungan data dan jaringan, tetapi juga bagian dari upaya menjaga kondisi kerja yang aman.

3.3. Strategi Pengamanan Sistem pada Otomasi Berbasis PLC

Keamanan sistem membutuhkan pengendalian terencana dari aspek teknologi, manusia, dan prosedur operasional. Pengamanan tidak cukup dengan antivirus atau kata sandi, tetapi harus berlapis agar setiap bagian sistem terlindungi. NIST SP 800-82 Rev. 3 menjelaskan bahwa pengamanan Operational Technology harus mempertimbangkan karakteristik sistem industri, terutama keselamatan, keandalan, dan ketersediaan proses operasional (Stouffer et al., 2023). Beberapa strategi yang dapat diterapkan adalah sebagai berikut.

a) Pengendalian Akses dan Autentikasi Pengguna

Pengendalian akses memastikan hanya pekerja berwenang yang dapat menggunakan atau mengubah sistem otomasi. Setiap operator, teknisi, dan administrator memiliki akun masing-masing dengan tingkat akses sesuai tanggung jawabnya. Operator cukup diberi akses untuk menjalankan dan memantau mesin, sedangkan perubahan program PLC hanya dilakukan teknisi atau administrator berwenang. Kata sandi harus memenuhi persyaratan keamanan dan tidak boleh dibagikan. Akses jarak jauh perlu dibatasi dan dilindungi dengan autentikasi yang sesuai. Prinsip least privilege mengurangi risiko penyalahgunaan karena setiap pengguna hanya memperoleh hak yang diperlukan untuk pekerjaannya.

b) Perlindungan Program dan Konfigurasi PLC

Program PLC menentukan urutan kerja, kondisi operasi, dan respons mesin terhadap sinyal sensor, sehingga harus dilindungi dari perubahan tidak sah maupun kesalahan pemrograman. Salah satu langkahnya adalah membuat cadangan (backup) program yang telah diuji dan dinyatakan benar. Setiap perubahan harus melalui persetujuan, pemeriksaan, pengujian, dan dokumentasi sebelum diterapkan pada mesin produksi. Program yang tersimpan juga dapat dibandingkan dengan program yang sedang digunakan untuk mendeteksi perubahan yang tidak sesuai. Jika ditemukan perubahan mencurigakan, mesin harus dievaluasi sebelum dioperasikan kembali. Langkah ini menjaga integritas program dan mencegah hilangnya fungsi pengamanan mesin.

c) Segmentasi dan Perlindungan Jaringan Industri

Segmentasi jaringan memisahkan jaringan berdasarkan fungsi dan kebutuhan akses. Jaringan PLC sebaiknya dipisahkan dari jaringan perkantoran dan internet yang tidak berkaitan langsung dengan pengendalian mesin, misalnya menggunakan firewall industri, jaringan terpisah, dan pengaturan komunikasi sesuai kebutuhan operasional. Komputer administrasi, misalnya, tidak seharusnya dapat mengubah program PLC secara langsung. Komunikasi antara PLC, HMI, dan SCADA dibatasi hanya pada perangkat yang memerlukan pertukaran data. Dengan demikian, jika satu jaringan terganggu atau diserang, dampaknya tidak langsung menyebar ke seluruh sistem otomasi.

d) Pemantauan Aktivitas dan Deteksi Gangguan

Pemantauan bertujuan mengetahui kondisi perangkat, komunikasi jaringan, dan perubahan selama proses produksi. Pemantauan dapat berupa pencatatan aktivitas pengguna

(user activity logging), pemeriksaan perubahan program PLC, pemantauan status komunikasi, dan sistem deteksi anomali jaringan. Sistem ini membantu mengidentifikasi aktivitas tidak biasa, seperti percobaan akses berulang, perubahan program di luar jadwal pemeliharaan, atau komunikasi dari perangkat tidak dikenal. Jika ditemukan aktivitas mencurigakan, petugas bertanggung jawab melakukan pemeriksaan dan bertindak sesuai prosedur penanganan insiden. Pemantauan yang konsisten membantu mendeteksi gangguan lebih awal sebelum berkembang menjadi kegagalan sistem yang membahayakan pekerja.

e) Pemeliharaan dan Pembaruan Keamanan Sistem

Pemeliharaan keamanan memastikan perangkat keras dan lunak otomasi tetap berfungsi optimal. Kegiatannya mencakup pemeriksaan komputer pemrograman, pengujian perangkat komunikasi, pembaruan perangkat lunak, pemeriksaan konfigurasi, dan evaluasi kerentanan. Pembaruan keamanan (security patch) perlu dilakukan terencana dengan mempertimbangkan kompatibilitas perangkat dan kebutuhan operasional, karena pembaruan yang tidak diuji dapat mengganggu komunikasi atau menyebabkan ketidakstabilan sistem kontrol. Pembaruan sebaiknya diuji pada lingkungan yang sesuai dan diterapkan melalui prosedur perubahan yang disetujui. Salinan cadangan program dan konfigurasi juga harus tersedia agar sistem dapat dipulihkan jika terjadi kegagalan.

f) Penerapan Keamanan Fisik Perangkat PLC

Keamanan fisik mencegah orang tidak berwenang mengakses perangkat kontrol secara langsung. Panel PLC, komputer pemrograman, switch jaringan, dan perangkat pengendali lainnya harus ditempatkan di area dengan akses terbatas. Panel kontrol sebaiknya dikunci dan hanya dapat dibuka teknisi berwenang. Kabel komunikasi dan perangkat penyimpanan juga perlu dilindungi dari kerusakan maupun penggunaan tanpa izin. Penggunaan flashdisk atau perangkat eksternal pada komputer pemrograman harus dikendalikan karena dapat menjadi jalur masuk perangkat lunak berbahaya. Keamanan fisik menjadi langkah penting untuk melindungi sistem dari gangguan yang berasal dari lingkungan kerja.

g) Pelatihan dan Peningkatan Kesadaran Keamanan Pekerja

Pekerja merupakan unsur penting dalam keamanan sistem karena sebagian besar aktivitas operasional melibatkan interaksi manusia dengan perangkat otomasi. Operator dan teknisi perlu dilatih mengenai penggunaan PLC, pengelolaan kata sandi, pengenalan aktivitas mencurigakan, prosedur perubahan program, dan penanganan gangguan sistem. Mereka juga harus memahami bahwa menonaktifkan sensor pengaman, menggunakan akun orang lain, atau menghubungkan perangkat eksternal tanpa izin dapat membahayakan keselamatan kerja. Pelatihan dilakukan berkala agar pekerja mampu mengenali ancaman dan bertindak tepat. Dengan demikian, keamanan sistem tidak hanya bergantung pada teknologi, tetapi juga pada kedisiplinan dan kesadaran seluruh pekerja.

Berdasarkan kajian literatur, bahaya pada sistem otomasi dapat berasal dari aspek listrik, mekanik, manusia, prosedur, dan sistem kendali. Pada praktikum PLC, bahaya listrik dapat muncul dari terminal bertegangan, kabel terkelupas, hubungan singkat, atau pengawatan yang salah. Bahaya mekanik dapat terjadi ketika output PLC mengaktifkan motor, solenoid, silinder pneumatik, atau mekanisme lain secara tiba-tiba. Sementara itu, bahaya akibat faktor manusia dapat muncul karena kurangnya pemeriksaan, salah memahami diagram, salah memasukkan alamat I/O, atau menjalankan program tanpa memastikan kondisi mesin. Penelitian ’Adil et al. (2025) memperlihatkan pentingnya penilaian risiko pada teknologi otomasi berbasis PLC. Sistem otomasi perlu dinilai berdasarkan kejadian berbahaya yang mungkin terjadi, kemudian dilakukan pengurangan risiko melalui solusi teknis. Pendekatan tersebut relevan untuk praktikum karena trainer PLC dapat dianggap sebagai sistem otomasi skala laboratorium. Artinya, sebelum sistem dijalankan, mahasiswa perlu memastikan bahwa bagian yang bergerak, sumber energi, rangkaian listrik, dan fungsi kontrol berada dalam kondisi aman.

No	Aktivitas/kondisi	Potensi Bahaya	Dampak	Pengendalian yang disarankan
1	Pengawatan PLC	Sengatan Listrik/hubungan singkat	Cedera atau kerusakan komputer	Pastikan sumber OFF, periksa kabel dan terminal, gunakan SOP
2	Mengubah program saat 9ystem siap berjalan	Output aktif tidak terduga	Aktuator bergerak dan mencederai pengguna	Hentikan sistem,verifikasi program, dan lakukan uji bertahap
3	Pengujian Output	Motor/solenoid bergerak tiba-tiba	Terjepit/terbentur atau kerusakan alat	Area gerak diberi batas, gunakan mode uji aman dan emergency stop
4	Kabel tidak tertata	Salah sambung/tersandung	Gangguan fungsi dan cedera	Label kabel, rapikan jalur, gunakan terminal sesuai diagram
5	Tidak menggunakan SOP/APD	Kesalahan prosedur	Meningkatkan peluang kecelakaan	Briefing, SOP, Pengawasan, dan APD sesuai risiko

Table 1 Indentifikasi bahaya dan pengendalian pada praktikum PLC

Kesalahan pertama yang perlu dikurangi adalah melakukan pengawatan atau perubahan rangkaian tanpa memastikan sumber energi dalam kondisi aman. Kondisi ini dapat menyebabkan kontak dengan bagian bertegangan atau hubungan singkat. Kesalahan kedua adalah menguji program secara langsung pada aktuator tanpa pemeriksaan urutan logika. Program yang salah alamat input/output, salah kondisi *interlock*, atau salah urutan kerja dapat mengaktifkan output yang tidak diharapkan. Kesalahan ketiga adalah tidak melakukan inspeksi visual terhadap kabel, terminal, konektor, dan komponen sebelum sistem dihidupkan.

Kesalahan berikutnya berkaitan dengan pengendalian gerakan. Pada sistem yang memiliki aktuator, operator tidak boleh menganggap bahwa berhentinya program berarti seluruh sumber energi mekanik telah hilang. Oleh karena itu, posisi aman, penghentian energi, dan fungsi penghentian darurat perlu dipastikan. Prinsip keselamatan mesin menempatkan pengendalian teknis sebagai bagian penting dari pengurangan risiko, sehingga prosedur kerja sebaiknya didukung oleh desain dan perangkat pengaman, bukan hanya mengandalkan kehati-hatian pengguna (’Adil et al., 2025).

Kesalahan dari sisi administrasi dapat berupa tidak adanya SOP, tidak adanya checklist pemeriksaan, kurangnya briefing, dan kurangnya pencatatan kejadian atau near miss. Penelitian mengenai penerapan prosedur dan pengetahuan K3 menunjukkan pentingnya prosedur kerja, pengetahuan, dan pelatihan dalam pencegahan kecelakaan. Dengan demikian, praktikum PLC perlu memasukkan K3 sebagai bagian dari langkah kerja, bukan sebagai materi tambahan setelah praktik selesai (Imasya Putri et al., 2021).

3.1. Penerapan K3 yang lebih baik

Penerapan K3 yang lebih baik dapat dimulai sebelum sistem diberi energi. Praktikan melakukan briefing singkat, mempelajari diagram rangkaian, mengenali sumber bahaya, memastikan komponen sesuai, dan memeriksa kondisi kabel. Setelah pengawatan selesai, pemeriksaan dilakukan oleh praktikan dan, bila memungkinkan, diverifikasi oleh instruktur sebelum power dinyalakan. Program PLC juga sebaiknya diuji terlebih dahulu dengan kondisi yang paling aman, misalnya memeriksa status input dan output melalui simulator atau indikator sebelum menghubungkan aktuator yang memiliki gerakan.

Pengendalian teknis perlu diprioritaskan ketika risiko tidak cukup dikurangi melalui prosedur. Contohnya adalah pemasangan pelindung pada bagian bergerak, penggunaan emergency stop, pembatasan akses area gerak, penggunaan power supply dan proteksi yang sesuai, serta interlock agar kondisi tertentu tidak dapat menjalankan aktuator secara berbahaya. Konsep pengurangan risiko pada ISO 12100 menempatkan desain aman dan pengamanan teknis sebagai unsur penting sebelum mengandalkan peringatan atau instruksi penggunaan.

Dari sisi administrasi, laboratorium sebaiknya mempunyai SOP khusus untuk pengawatan, pemrograman, pengujian, troubleshooting, dan penghentian sistem. Checklist sebelum operasi dapat berisi pemeriksaan sumber listrik, kabel, terminal, grounding bila relevan, alamat I/O, kondisi aktuator, tombol stop/emergency stop, dan area kerja. Setelah praktikum, sistem dikembalikan ke kondisi aman dan sumber energi dimatikan.

Penggunaan APD harus disesuaikan dengan hasil penilaian risiko dan aturan laboratorium. APD bukan pengganti pengendalian teknis, tetapi merupakan lapisan perlindungan tambahan. Penelitian HIRARC pada lingkungan laboratorium menunjukkan bahwa pengendalian dapat mencakup fasilitas keselamatan, pelatihan, tata letak, APD, dan SOP secara terpadu (Mahendra et al., 2025).

3.2.Rekomendasi SOP Singkat Praktikum PLC

1. Lakukan briefing K3 dan identifikasi bahaya sebelum praktik.
2. Pastikan sumber listrik dalam kondisi OFF ketika melakukan pengawatan atau perubahan rangkaian.
3. Periksa kabel, terminal, konektor, power supply, dan kondisi fisik trainer.
4. Cocokkan pengawatan dengan diagram dan beri identitas pada kabel/input-output.
5. Verifikasi program dan alamat I/O sebelum mengaktifkan aktuator.
6. Pastikan area gerak aktuator bebas dari tangan atau benda yang dapat mengganggu.
7. Gunakan interlock dan fungsi penghentian yang sesuai dengan sistem praktik.
8. Aktifkan sistem secara bertahap dan hentikan pengujian bila ditemukan kondisi tidak normal.
9. Catat kesalahan, gangguan, dan near miss sebagai bahan evaluasi.
10. Setelah selesai, matikan sumber energi dan kembalikan area kerja dalam kondisi aman.

3.3.Matriks Prioritas Pengendalian

Prioritas	Bentuk Pengendalian	Contoh pada PLC	Tujuan
1	Eliminasi/Substitusi	Menghilangkan Langkah kerja yang tidak diperlukan atau menggunakan sumber energi/komponen yang lebih aman bila memungkinkan	Mengurangi sumber bahaya

2	Rekayasa Teknik	Guard, Interlock, emergency stop, pembatas area gerak, proteksi listrik	Mencegah paparan bahaya
3	Administratif	SOP, checklist, briefing, pelatihan. Izin/otorisasi pengujian	Mengendalikan cara kerja
4	APD	APD sesuai resiko dan ketentuan laboratorium	Perlindungan tambahan

Table 2 Prioritas pengendalian risiko pada praktikum PLC

3.4.Pembahasan

Analisis Bentuk Human Error pada Sistem Otomasi Berbasis PLC

Penerapan sistem otomasi berbasis Programmable Logic Controller (PLC) tidak sepenuhnya menghilangkan keterlibatan manusia dalam proses produksi. Operator dan teknisi tetap memiliki tanggung jawab dalam mengoperasikan mesin, memantau kondisi sistem, melakukan pengaturan program, serta melaksanakan pemeliharaan. Dalam pelaksanaannya, kesalahan manusia (*human error*) dapat terjadi akibat kurangnya pemahaman terhadap sistem, kelalaian, tekanan pekerjaan, maupun ketidaksesuaian dalam menjalankan prosedur keselamatan. Kesalahan tersebut dapat menyebabkan gangguan pada proses otomasi dan menimbulkan risiko kecelakaan kerja apabila tidak dikendalikan dengan baik.

Beberapa bentuk *human error* yang dapat terjadi pada sistem otomasi berbasis PLC adalah sebagai berikut.

a) **Kesalahan Pengoperasian Mesin**

Kesalahan pengoperasian terjadi ketika operator menjalankan mesin tanpa memahami urutan kerja, fungsi tombol, atau kondisi keselamatan yang harus dipenuhi. Contohnya, operator menekan tombol *start* ketika area kerja masih terdapat pekerja atau benda yang menghalangi pergerakan aktuator. Kesalahan tersebut dapat menyebabkan mesin bergerak secara tiba-tiba dan berpotensi menimbulkan cedera, seperti terjepit atau tertimpa komponen mesin. Oleh karena itu, operator harus memahami prosedur pengoperasian dan memastikan kondisi area kerja aman sebelum menjalankan mesin.

b) **Kesalahan Pemrograman PLC**

Kesalahan pemrograman dapat dilakukan oleh teknisi ketika menyusun atau mengubah logika kontrol PLC tanpa melakukan pemeriksaan dan pengujian terlebih dahulu. Contohnya, kesalahan dalam membuat logika *interlock* menyebabkan mesin tetap dapat beroperasi meskipun pelindung mesin terbuka. Kondisi tersebut dapat menghilangkan fungsi pengamanan dan meningkatkan risiko kecelakaan. Untuk mencegahnya, setiap perubahan program harus melalui proses pemeriksaan, pengujian, pencadangan program, serta persetujuan dari petugas yang berwenang.

c) **Kelalaian dalam Menjalankan Prosedur Keselamatan**

Kelalaian dapat terjadi ketika pekerja mengabaikan SOP, tidak menggunakan alat pelindung diri (APD), atau melakukan pemeriksaan mesin tanpa mematikan sumber energi. Sebagai contoh, teknisi melakukan perbaikan pada mesin press hidrolik hanya dengan menekan tombol *stop*, tanpa memutus sumber listrik dan membuang tekanan hidrolik yang tersimpan. Akibatnya, mesin masih memiliki energi berbahaya yang dapat menyebabkan aktuator bergerak secara tidak terduga. Kondisi tersebut menunjukkan pentingnya penerapan prosedur *Lockout-Tagout* (LOTO) sebelum kegiatan perawatan atau perbaikan dilakukan.

d) **Kesalahan dalam Membaca Informasi Sensor dan HMI**

Kesalahan ini terjadi ketika operator salah memahami informasi yang ditampilkan pada *Human Machine Interface* (HMI), seperti indikator tekanan, suhu, posisi aktuator, maupun alarm gangguan. Contohnya, operator mengabaikan alarm tekanan berlebih karena menganggapnya sebagai gangguan biasa. Apabila kondisi tersebut tidak segera ditangani, mesin dapat terus beroperasi dalam keadaan tidak aman dan meningkatkan kemungkinan kerusakan maupun kecelakaan kerja. Oleh sebab itu, operator perlu memahami arti setiap indikator dan alarm serta mengikuti prosedur penanganan ketika sistem menunjukkan kondisi abnormal.

e) **Kesalahan dalam Pemeliharaan dan Pengamanan Sistem**

Kesalahan pemeliharaan dapat berupa tidak melakukan pemeriksaan berkala, menggunakan komponen pengganti yang tidak sesuai, atau menonaktifkan sensor dan perangkat pengaman tanpa prosedur yang benar. Contohnya, teknisi menonaktifkan sensor keselamatan agar proses produksi tetap berjalan ketika sensor mengalami gangguan. Tindakan tersebut dapat menyebabkan mesin tetap beroperasi meskipun kondisi keselamatannya belum terpenuhi. Untuk mencegah hal tersebut, kegiatan pemeliharaan harus dilakukan berdasarkan SOP, disertai pemeriksaan fungsi perangkat keselamatan sebelum mesin kembali dioperasikan.

Analisis hubungan Human Error dengan Risiko K3

Berdasarkan bentuk-bentuk kesalahan tersebut, dapat diketahui bahwa *human error* memiliki hubungan langsung dengan risiko K3 pada sistem otomasi berbasis PLC. Kesalahan manusia tidak selalu disebabkan oleh kelalaian individu, tetapi juga dapat dipengaruhi oleh kurangnya pelatihan, prosedur yang tidak jelas, beban kerja, desain antarmuka yang kurang mudah dipahami, dan lemahnya pengawasan. Oleh karena itu, perusahaan perlu menerapkan pengendalian melalui pelatihan operator dan teknisi, penyediaan SOP yang mudah dipahami, pembatasan hak akses program PLC, pemeriksaan berkala, serta penerapan LOTO. Selain itu, fungsi keselamatan seperti *emergency stop*, sensor pengaman, dan *safety interlock* harus diuji secara berkala agar tetap bekerja sesuai fungsinya. Dengan demikian, pengendalian *human error* merupakan bagian penting dalam penerapan K3 pada sistem otomasi berbasis PLC. Teknologi otomasi yang canggih tetap membutuhkan pekerja yang kompeten, prosedur yang tepat, dan sistem pengawasan yang memadai. Integrasi antara pengendalian risiko, peningkatan kompetensi manusia, dan keamanan sistem dapat mengurangi kemungkinan terjadinya kecelakaan kerja serta menjaga keandalan proses produksi.

Bentuk human error	Contoh kejadian	Risiko terhadap K3
Kesalahan pengoperasian	Menjalankan mesin ketika area kerja belum aman	Pekerja terjepit atau tertimpa
Kesalahan pemrograman	Logika interlock tidak berfungsi	Mesin bergerak dalam kondisi berbahaya
Kelalaian prosedur	Perbaikan tanpa penerapan LOTO	Terkena energi listrik atau gerakan aktuator
Kesalahan membaca HMI	Mengabaikan alarm tekanan berlebih	Kerusakan mesin dan kecelakaan kerja
Kesalahan pemeliharaan	Menonaktifkan sensor pengaman	Hilangnya fungsi perlindungan mesin

Table 2 Identifikas bentuk pada praktikum PLC

Hasil kajian menunjukkan bahwa penerapan K3 pada PLC dan sistem kendali harus dipandang sebagai pengendalian sistem secara menyeluruh. Keselamatan tidak cukup hanya dengan menggunakan APD atau memasang tanda peringatan. Risiko perlu dikurangi mulai

dari desain, pengamanan teknis, prosedur, kompetensi operator, hingga evaluasi setelah praktik. Hal ini sejalan dengan penelitian ’Adil et al. (2025) yang menggunakan penilaian risiko internal dan retrofit untuk menurunkan risiko pada otomasi berbasis PLC.

Penggunaan HIRARC dapat membantu mahasiswa memahami bahwa setiap langkah kerja mempunyai bahaya dan tingkat risiko yang berbeda. Sebagai contoh, pengawatan ketika power OFF mempunyai risiko yang lebih rendah dibanding pengawatan ketika power ON. Demikian pula pengujian lampu indikator lebih sederhana dibanding pengujian motor atau aktuator. Oleh karena itu, pengendalian harus disesuaikan dengan karakteristik pekerjaan dan konsekuensi kegagalannya.

Pada konteks pendidikan vokasi, penerapan K3 juga berfungsi membentuk kebiasaan kerja industri. Mahasiswa tidak hanya dituntut mampu membuat program PLC yang bekerja, tetapi juga mampu menjelaskan sumber bahaya, melakukan pemeriksaan sebelum operasi, mengikuti SOP, dan menghentikan proses ketika ditemukan kondisi tidak aman. Dengan pendekatan tersebut, keberhasilan praktikum tidak hanya diukur dari sistem yang berhasil menyala, tetapi juga dari kemampuan menjalankan sistem secara aman dan terkendali.

4. KESIMPULAN

Penerapan K3 pada praktikum PLC dan sistem kendali perlu dilakukan terintegrasi, mulai dari identifikasi bahaya, penilaian risiko, pengendalian teknis, prosedur kerja, penggunaan APD, hingga evaluasi. Kesalahan yang perlu diperhatikan meliputi pengawatan saat sumber masih aktif, kabel dan terminal yang tidak diperiksa, kesalahan alamat I/O atau logika program, pengujian aktuator tanpa memastikan area aman, serta kurangnya SOP dan checklist. Pendekatan HIRARC dan prinsip ISO 12100 dapat menjadi dasar untuk mengenali dan mengendalikan risiko tersebut.

Perbaikan yang direkomendasikan meliputi briefing dan pemeriksaan sebelum praktik, pemastian sumber energi aman saat pengawatan, verifikasi program sebelum aktuator dijalankan, penyediaan emergency stop dan interlock, penjagaan area gerak, penerapan SOP dan checklist, serta pencatatan kesalahan dan near miss. Dengan demikian, praktikum PLC tidak hanya menghasilkan sistem kendali yang berfungsi, tetapi juga membentuk budaya kerja yang aman dan bertanggung jawab.

Human error juga menjadi faktor penting karena kesalahan pengoperasian, pemrograman, pembacaan informasi HMI, kelalaian prosedur, dan kesalahan pemeliharaan dapat membuat sistem bekerja dalam kondisi tidak aman. Oleh karena itu, diperlukan peningkatan kompetensi operator dan teknisi, pelatihan, kepatuhan terhadap SOP, serta pengawasan berkala. Keamanan sistem turut berperan menjaga keselamatan pekerja, sebab akses tidak sah, manipulasi program PLC, malware, dan gangguan komunikasi dapat memengaruhi pengendalian mesin. Pembatasan hak akses, pencadangan program, pemantauan aktivitas, perlindungan jaringan, dan pemeriksaan fungsi perangkat keselamatan perlu diterapkan secara berkelanjutan.

Dengan demikian, penerapan K3 pada sistem otomasi berbasis PLC harus memperhatikan tiga aspek utama, yaitu pengendalian risiko, pengendalian human error, dan keamanan sistem, yang saling berkaitan dalam menciptakan sistem otomasi yang aman, andal, dan produktif tanpa mengabaikan keselamatan dan kesehatan pekerja.

5. UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Jurusan Teknik Mesin, Politeknik Negeri Subang, atas dukungan, fasilitas, dan kesempatan yang diberikan selama kegiatan pembelajaran dan penyusunan kajian ini. Penulis juga berterima kasih kepada dosen pengampu mata kuliah atas bimbingan, arahan, dan masukan yang membantu penulis memahami konsep keselamatan dan kesehatan kerja pada sistem otomasi berbasis PLC.

Ucapan terima kasih juga disampaikan kepada para peneliti, penulis, dan lembaga penyusun standar yang karyanya menjadi rujukan dalam kajian literatur ini. Selain itu, penulis berterima kasih kepada rekan-rekan mahasiswa dan semua pihak yang telah memberikan bantuan, diskusi, dan dukungan, baik secara langsung maupun tidak langsung, sehingga jurnal ini dapat diselesaikan

dengan baik. Semoga kajian ini bermanfaat bagi pengembangan ilmu pengetahuan dan penerapan K3 di bidang teknik.

DAFTAR PUSTKA

a) 'Adil, N. M. M., Saputro, R. D. A., & Ashari, F. (2025). Mechanical hazard simulator of PLC-based automation technology according to ISO 12100. Jurnal E-Komtek, 9(2), 593–600. https://doi.org/10.37339/e-komtek.v9i2.2834
b) Cusimano, J. (2022). Industrial control system risk assessment standards and leading practices in the chemical industry. Process Safety Progress, 41(4), 665–669. https://doi.org/10.1002/prs.12372
c) Imasya Putri, A. S. R., Wahyu, A., & Thamrin, Y. (2021). Penerapan prosedur dan pengetahuan K3 terhadap kejadian kecelakaan kerja pada pekerja PT. Industri Kapal Indonesia. Hasanuddin Journal of Public Health, 2(2).
d) Mahendra, G., Sofitra, M., & Uslianti, S. (2025). Analisis potensi bahaya dan usulan perbaikan pada laboratorium jurusan teknik industri dan teknik lingkungan menggunakan metode HIRARC. Jurnal Teknik Industri Universitas Tanjungpura, 9(1).
e) Obele, A. F., Aikhuele, D. O., & Nwosu, H. U. (2024). A review of reliability techniques for the evaluation of Programmable Logic Controller. World Journal of Electrical and Electronic Engineering, 3(1), 24–57. https://doi.org/10.31586/wjeee.2024.947
f) Widana, A. K., Wiryajati, I. K., & Adnyani, I. A. S. (2024). Identifikasi bahaya dan penilaian risiko keselamatan dan kesehatan kerja menggunakan metode HIRARC pada Gardu Induk Ampenan. Jurnal Informatika dan Teknik Elektro Terapan, 12(3S1), 4129–4136. https://doi.org/10.23960/jitet.v12i3S1.5272
g) Stouffer, K., Pease, M., Tang, C., Zimmerman, T., Pillitteri, V., Lightman, S., Hahn, A., Saravia, S., Sherule, A., & Thompson, M. (2023). *Guide to Operational Technology (OT) Security (NIST Special Publication 800-82 Rev. 3)*. National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3
h) International Society of Automation. (2025). *ISA/IEC 62443 Series of Standards: Security for Industrial Automation and Control Systems.* ISA. Sumber resmi ISA/IEC 62443.
i) Cybersecurity and Infrastructure Security Agency. (n.d.). *Cybersecurity Best Practices for Industrial Control Systems.* CISA. Dokumen rekomendasi keamanan ICS dari CISA.
j) International Society of Automation. (2020). *ANSI/ISA-62443-3-2-2020: Security for Industrial Automation and Control Systems – Security Risk Assessment for System Design.* ISA. Dokumen ISA-62443-3-2.
k) Stouffer, K., et al. (2023). *Guide to Operational Technology (OT) Security (NIST Special Publication 800-82 Rev. 3).* National Institute of Standards and Technology. https://doi.org/10.6028/NIST.SP.800-82r3.
l) NIST Computer Security Resource Center+1
International Society of Automation. (2020). *ANSI/ISA-62443-3-2-2020: Security for Industrial Automation and Control Systems – Security Risk Assessment for System Design.* ISA. Akses dokumen ISA (PDF).
m) Powell, M., et al. (2022). *Protecting Information and System Integrity in Industrial Control System Environments: Cybersecurity for the Manufacturing Sector (NIST SP 1800-10).* National Institute of Standards and Technology. Akses dokumen NIST