

**ANALISIS PEMAHAMAN CYBERSECURITY DAN SYSTEM OTOMASI
TERHADAP KESIAPAN KERJA DI INDUSTRI OTOMASI PADA MAHASISWA
PROGRAM STUDI PENDIDIKAN VOKASIONAL MEKATRONIKA
UNIVERSITAS NEGERI MAKASSAR**

Astryd Dwi Apriliani¹, Muh Ma'ruf Idris², Edy Sabara³

¹²³JTETI FT Universitas Negeri Makassar

1astryddwiapriliani064@gmail.com, 2maruf.idris@unm.ac.id, 3edysabara66@unm.ac.id

ABSTRACT

Astryd Dwi Apriliani. 2026. Analysis of Cybersecurity and Automation Systems Understanding on Work Readiness in the Automation Industry among Students of the Vocational Mechatronics Education Study Program, Universitas Negeri Makassar. Undergraduate Thesis. Faculty of Engineering, Universitas Negeri Makassar. (Supervised by Muh. Ma'ruf Idris and Edy Sabara).

This study aims to determine the level of students' understanding of cybersecurity and automation systems and to analyze the influence of both variables on the work readiness of students in the Vocational Mechatronics Education Study Program at Universitas Negeri Makassar for the automation industry. This research employed a quantitative approach with a descriptive correlational design. The sample consisted of 85 students selected using a saturated sampling (total sampling) technique. Data were collected through questionnaires and analyzed using descriptive statistics, validity and reliability tests, prerequisite tests, Pearson correlation analysis, and multiple linear regression with the assistance of SPSS software. The results indicated that the research instruments were valid and reliable. Furthermore, cybersecurity understanding and automation systems understanding had a positive and significant effect on students' work readiness, both partially and simultaneously. These findings indicate that a higher level of understanding of cybersecurity and automation systems is associated with better work readiness to meet the demands of the automation industry. Therefore, strengthening cybersecurity and automation systems education in vocational programs is essential to prepare competent graduates who are ready to face the challenges of modern industry.

Keywords: Cybersecurity, Automation Systems, Work Readiness.

ABSTRAK

Analisis Pemahaman Cybersecurity dan Sistem Otomasi Terhadap Kesiapan Kerja di Industri Otomasi Pada Mahasiswa Program Studi Pendidikan Vokasional Mekatronika Universitas Negeri Makassar. **Skripsi Fakultas Teknik Universitas Negeri Makassar** (dibimbing oleh Muh. Ma'ruf Idris dan Edy Sabara)

Penelitian ini bertujuan untuk mengetahui tingkat pemahaman cybersecurity dan sistem otomasi serta menganalisis pengaruh keduanya terhadap kesiapan kerja mahasiswa Program Studi Pendidikan Vokasional Mekatronika Universitas Negeri Makassar di industri otomasi. Penelitian ini menggunakan pendekatan kuantitatif dengan desain deskriptif korelasional. Sampel penelitian berjumlah 85 mahasiswa

yang ditentukan menggunakan teknik sampling jenuh (total sampling). Data dikumpulkan melalui kuesioner dan dianalisis menggunakan statistik deskriptif, uji validitas, uji reliabilitas, uji prasyarat analisis, korelasi Pearson, dan regresi linear berganda dengan bantuan SPSS. Hasil penelitian menunjukkan bahwa instrumen penelitian memenuhi kriteria valid dan reliabel. Selain itu, pemahaman cybersecurity dan pemahaman sistem otomasi berpengaruh positif dan signifikan terhadap kesiapan kerja mahasiswa, baik secara parsial maupun simultan. Temuan ini menunjukkan bahwa semakin baik pemahaman mahasiswa mengenai cybersecurity dan sistem otomasi, semakin tinggi kesiapan kerja mereka dalam menghadapi tuntutan industri otomasi. Oleh karena itu, penguatan pembelajaran cybersecurity dan sistem otomasi perlu terus dikembangkan dalam pendidikan vokasional untuk menghasilkan lulusan yang kompeten dan siap menghadapi perkembangan industri.

Kata kunci: Cybersecurity, Sistem Otomasi, Kesiapan Kerja

A. Pendahuluan

Era transformasi digital dan Revolusi Industri 4.0 telah membawa perubahan paradigmat yang sangat masif pada sektor manufaktur global melalui integrasi teknologi digital dan fisik secara real-time. Perkembangan ini melahirkan konsep smart factory, di mana sistem produksi modern tidak lagi berdiri sendiri, melainkan saling terhubung secara digital melalui teknologi Internet of Things (IoT), Supervisory Control and Data Acquisition (SCADA), serta sistem kontrol berbasis komputer. Integrasi yang intensif ini meningkatkan efisiensi operasional secara signifikan, namun di sisi lain juga membuka celah kerentanan baru terhadap ancaman keamanan digital. Berdasarkan laporan IBM Security X-

Force (2022), sektor manufaktur kini telah menjadi target serangan siber terbanyak secara global, dengan dampak destruktif yang bervariasi mulai dari pencurian data, gangguan operasional jalur produksi, hingga kerugian finansial yang masif. Kondisi ini menegaskan bahwa keamanan informasi di industri modern bukan lagi sekadar persoalan proteksi teknologi informasi (TI) konvensional, melainkan aspek krusial yang menentukan keberlanjutan proses otomasi itu sendiri.

Meskipun literasi digital mahasiswa di Indonesia secara umum tergolong tinggi, kesadaran dan pengetahuan taktis mengenai perlindungan siber (cybersecurity awareness) pada sistem infrastruktur fisik di kalangan mahasiswa teknik

masih perlu ditingkatkan secara signifikan. Fenomena kesenjangan ini menjadi sangat relevan dalam lingkup pendidikan vokasional, khususnya pada Program Studi Pendidikan Vokasional Mekatronika Universitas Negeri Makassar. Pada tingkat ini, mahasiswa secara rutin berinteraksi dengan sistem laboratorium teknik, sistem kontrol berbasis Programmable Logic Controller (PLC), sensor, aktuator, serta modul komunikasi industri. Di tengah tuntutan industri yang dinamis, pemahaman mahasiswa vokasi mengenai perlindungan digital sering kali masih terbatas pada aspek keamanan komputer dasar atau administratif, dan belum menyentuh aspek pertahanan yang kompleks pada sistem kontrol industri terdistribusi. Padahal, kegagalan dalam mengidentifikasi kerentanan sistem yang dioperasikan berpotensi memicu kegagalan sistem kontrol fisik yang fatal bagi operasional industri otomasi.

Di sisi lain, penguasaan terhadap konsep dan praktikum sistem otomasi industri tetap menjadi kompetensi inti yang wajib dipenuhi oleh setiap lulusan mekatronika. Otomasi industri merupakan pilar

utama manufaktur cerdas yang beroperasi secara otomatis dengan meminimalkan keterlibatan manual manusia guna mencapai produktivitas, konsistensi kualitas, dan efisiensi energi yang optimal. Kurikulum pendidikan mekatronika dituntut untuk senantiasa adaptif terhadap perkembangan teknologi perangkat keras maupun perangkat lunak terbaru. Kendati demikian, keterbatasan sarana laboratorium serta lambatnya pembaruan kurikulum di tingkat perguruan tinggi kerap menghambat peningkatan literasi otomasi mahasiswa pada ranah integrasi digital yang mendalam. Akibatnya, kesiapan kerja mahasiswa dalam menghadapi tuntutan nyata industri modern sering kali terhambat akibat tidak sinkronnya keahlian teknis konvensional dengan dinamika perkembangan siber industri di kancah global.

Kesiapan kerja mahasiswa itu sendiri merupakan konstruksi yang dipengaruhi oleh kombinasi kemampuan teknis (*hard skills*), kemampuan non-teknis (*soft skills*), literasi digital, dan etos kerja yang dibentuk selama masa perkuliahan. Lulusan mekatronika di era sekarang tidak hanya dituntut

memiliki kemampuan merancang program logika PLC atau mendesain antarmuka HMI yang andal, melainkan juga harus memiliki bekal pengetahuan protektif untuk memastikan keamanan fungsionalitas sistem tersebut dari ancaman disrupsi luar. Namun, hingga saat ini, belum terdapat kajian empiris yang secara spesifik memetakan tingkat pemahaman cybersecurity dan pengetahuan sistem otomasi industri serta pengaruhnya secara simultan maupun parsial terhadap kesiapan kerja di industri otomasi pada mahasiswa Pendidikan Vokasional Mekatronika UNM. Adanya kekosongan data empiris ini menyulitkan evaluasi efektivitas kurikulum pembelajaran vokasional dalam menyesuaikan diri dengan profil kompetensi yang dibutuhkan oleh pasar kerja industri saat ini.

Berdasarkan permasalahan nyata tersebut, penelitian ini

dilaksanakan dengan fokus untuk menganalisis hubungan sebab-akibat antar-variabel secara kuantitatif. Penelitian ini secara khusus bertujuan untuk mengetahui tingkat pemahaman cybersecurity mahasiswa, memetakan tingkat pemahaman sistem otomasi industri, serta menganalisis seberapa besar pengaruh pemahaman cybersecurity dan pemahaman sistem otomasi baik secara parsial maupun simultan terhadap kesiapan kerja mahasiswa Pendidikan Vokasional Mekatronika Universitas Negeri Makassar di industri otomasi. Temuan dan hasil penelitian ini diharapkan dapat memberikan kontribusi teoritis bagi pengembangan literatur integrasi keamanan siber dalam kurikulum teknik terapan, serta memberikan masukan praktis bagi institusi pendidikan vokasi dalam merumuskan strategi pengajaran yang lebih responsif dan relevan dengan tantangan ekosistem kerja digital.

B. Metode Penelitian

Penelitian ini menggunakan pendekatan kuantitatif dengan desain deskriptif korelasional (asosiatif). Pendekatan deskriptif digunakan untuk memberikan gambaran objektif mengenai tingkat pemahaman *cybersecurity*, tingkat pemahaman sistem otomasi industri, serta kesiapan kerja mahasiswa. Sementara itu, pendekatan asosiatif korelasional diterapkan untuk menganalisis hubungan dan menguji pengaruh secara empiris antara variabel bebas terhadap variabel terikat. Variabel bebas dalam penelitian ini adalah pemahaman *cybersecurity* (X_1) dan pemahaman sistem otomasi (X_2), sedangkan variabel terikat adalah kesiapan kerja mahasiswa di industri otomasi (Y).

Penelitian ini dilaksanakan di Program Studi Pendidikan Vokasional Mekatronika, Jurusan Teknik Elektronika dan Teknologi Informasi, Fakultas Teknik, Universitas Negeri Makassar. Populasi penelitian ini mencakup seluruh mahasiswa aktif Program Studi Pendidikan Vokasional Mekatronika Angkatan 2022, 2023, dan 2024. Teknik pengambilan sampel yang digunakan adalah

sampling jenuh (*total sampling*), di mana seluruh anggota populasi yang memenuhi kriteria inklusi dijadikan sampel penelitian, dengan jumlah total responden sebanyak 85 mahasiswa. Kriteria inklusi mensyaratkan responden telah menempuh mata kuliah terkait sistem otomasi, sedangkan kriteria eksklusi berlaku bagi mahasiswa yang sedang cuti atau berstatus tidak aktif pada semester penelitian berjalan.

Data dikumpulkan menggunakan metode kuesioner (angket) tertutup dan dokumentasi. Angket disusun berdasarkan kisi-kisi indikator variabel yang mencakup:

1. **Pemahaman *Cybersecurity* (X_1):** Pemahaman konsep dasar *cybersecurity*, identifikasi jenis dan karakteristik ancaman siber, serta strategi pengamanan sistem.
2. **Pemahaman Sistem Otomasi (X_2):** Pemahaman konsep dasar otomasi industri, prinsip kerja dan pemrograman PLC, fungsi dan penerapan SCADA dan HMI, serta integrasi *Internet of Things* (IoT).
3. **Kesiapan Kerja (Y):** Kemampuan menerapkan pengetahuan teknis, kesiapan

keterampilan operasional, serta kesiapan mental dan adaptasi terhadap lingkungan industri.

Setiap butir pernyataan dalam kuesioner dinilai menggunakan Skala Likert 5 tingkat, yaitu: Sangat Setuju (skor 5), Setuju (skor 4), Ragu-ragu (skor 3), Tidak Setuju (skor 2), dan Sangat Tidak Setuju (skor 1).

Sebelum kuesioner digunakan untuk mengumpulkan data riil, dilakukan uji validitas instrumen menggunakan rumus korelasi *Product Moment Pearson*. Item pernyataan dinyatakan valid jika nilai $r_{hitung} > r_{tabel}$ ($r_{tabel} = 0,213$ untuk $N = 85$ pada taraf signifikansi 5%). Pengujian reliabilitas instrumen dilakukan menggunakan koefisien *Cronbach's Alpha* dengan batas reliabilitas minimal sebesar 0,60.

Teknik analisis data yang digunakan dalam penelitian ini meliputi:

1. Analisis Statistik Deskriptif:

Digunakan untuk mendeskripsikan sebaran data melalui nilai rata-rata (mean), nilai minimum, nilai maksimum, dan standar deviasi.

2. Uji Prasyarat Analisis: Meliputi uji normalitas menggunakan grafik *Normal P-P Plot*, uji

linearitas hubungan melalui *Scatterplot*, uji multikolinearitas (dengan melihat nilai *Tolerance* > 0,10 dan *VIF* < 10), serta uji heteroskedastisitas menggunakan uji *Glejser*.

3. Uji Hipotesis: Menggunakan analisis Korelasi Pearson untuk mengetahui arah hubungan, analisis korelasi ganda untuk melihat hubungan simultan, serta analisis Regresi Linear Berganda untuk menguji pengaruh secara parsial (Uji *t*) maupun secara simultan (Uji *F*) pada taraf signifikansi 5% ($\alpha = 0,05$) dengan bantuan perangkat lunak SPSS

C. Hasil Penelitian dan Pembahasan

Berdasarkan hasil uji validitas instrumen dengan nilai *r*-tabel 0,213 ($N = 85$), seluruh item pada variabel Pemahaman Cybersecurity (X_1), Pemahaman Sistem Otomasi (X_2), dan Kesiapan Kerja (Y) dinyatakan valid karena memiliki nilai *r*-hitung > *r*-tabel dan signifikansi 0,000 (< 0,05). Pengujian reliabilitas juga menunjukkan nilai *Cronbach's Alpha* yang andal (> 0,60), yaitu X_1 sebesar 0,804; X_2 sebesar 0,803; dan Y sebesar 0,792

Tabel 1 Ringkasan Hasil Uji Validitas Variabel Penelitian

Indikator	Rentang r-hitung	r-tabel
Pemahaman Cybersecurity (X_1)	0,760 - 0,876	0,213
Pemahaman Sistem Otomasi (X_2)	0,828 - 0,910	0,213
Kesiapan Kerja (Y)	0,690 - 0,919	0,213

Analisis statistik deskriptif terhadap 85 responden menunjukkan nilai rata-rata (mean) variabel X_1 sebesar 23,7294; variabel X_2 sebesar 28,0471; dan variabel Y sebesar 49,1294. Seluruh nilai rata-rata yang cenderung mendekati nilai maksimum data mengindikasikan tingkat pemahaman dan kesiapan kerja mahasiswa berada pada kategori yang baik. Hasil pengujian asumsi prasyarat analisis mengonfirmasi bahwa data residual berdistribusi normal, memiliki pola hubungan yang linear, terbebas dari multikolinearitas ($VIF\ 2,465 < 10$; *Tolerance* $0,406 > 0,10$), serta tidak mengalami gejala heteroskedastisitas (Sig. Glesjer $> 0,05$).

Analisis Korelasi Pearson membuktikan adanya hubungan positif yang kuat antara pemahaman *cybersecurity* dengan kesiapan kerja

($r = 0,740$) dan hubungan pemahaman sistem otomasi dengan kesiapan kerja ($r = 0,783$). Melalui pengujian korelasi ganda, hubungan gabungan X_1 dan X_2 secara simultan terhadap Y berkategori sangat kuat dengan koefisien korelasi R sebesar 0,834

Pada pembahasan analisis inferensial regresi linear berganda diperoleh temuan sebagai berikut:

1. Pengaruh Parsial X_1 terhadap

Y: Pemahaman *cybersecurity* terbukti berpengaruh positif dan signifikan terhadap kesiapan kerja secara parsial dengan nilai t_{hitung} 3,450 (Sig. $0,001 < 0,05$). Pengetahuan proteksi jaringan dan mitigasi ancaman digital membentuk kesiapan operasional mahasiswa di lingkungan *Cyber-Physical Systems*.

2. Pengaruh Parsial X_2 terhadap

Y: Pemahaman sistem otomasi berpengaruh positif dan signifikan secara parsial terhadap kesiapan kerja dengan nilai t_{hitung} 6,782 (Sig. $0,000 < 0,05$). Berdasarkan nilai *Standardized Coefficients Beta* ($\beta = 0,598$), variabel ini memiliki pengaruh paling besar dan dominan dalam menentukan kesiapan psikomotorik mahasiswa di industri manufaktur.

3. **Pengaruh Simultan (X_1 , X_2) terhadap Y:** Pengujian menggunakan uji F menghasilkan nilai F_{hitung} sebesar 93,838 dengan signifikansi 0,000 ($< 0,05$), yang berarti pemahaman *cybersecurity* dan sistem otomasi secara bersama-sama berpengaruh nyata terhadap kesiapan kerja mahasiswa. Kontribusi gabungan kedua variabel independen ini (R Square) adalah sebesar 69,6%, sedangkan sisanya 30,4% dipengaruhi faktor lain di luar model

D. Kesimpulan

Kesiapan kerja mahasiswa Program Studi Pendidikan Vokasional Mekatronika UNM dipengaruhi secara signifikan oleh pemahaman *cybersecurity* dan pemahaman sistem otomasi, baik secara mandiri maupun kolektif. Pemahaman sistem otomasi bertindak sebagai kualifikasi inti operasional teknik, sementara literasi *cybersecurity* menyempurnakannya sebagai proteksi sistem dari gangguan digital global. Disarankan kepada institusi pendidikan vokasi mekatronika untuk mempertahankan

integrasi aspek keamanan siber ke dalam kurikulum teknik otomasi guna mencetak lulusan manufaktur cerdas (*Smart Manufacturing*) yang adaptif dan berdaya saing tinggi.

DAFTAR PUSTAKA

Buku :

Hidayat, R. (2021). *Keamanan Siber dalam Sistem Otomasi Industri*. Deepublish.

Nugroho, S. (2022). *Cybersecurity dan IoT dalam Sistem Mekatronika Industri*. ITB Press.

Sugiyono. (2020). *Metode Penelitian Kuantitatif, Kualitatif, dan R&D*. Alfabeta.

Xynexis International. (2025). *Cybersecurity Education for Digital Workforce*. Xynexis.

Dokumen Regulasi:

Badan Siber dan Sandi Negara. (2023). *Laporan Tahunan Keamanan Siber Indonesia*. Badan Siber dan Sandi Negara.

BINUS University. (2024). *Kesiapan tenaga kerja di era revolusi industri 4.0*.

Bridgenr. (2024). *Otomasi industri*. <https://bridgenr.com/id/blog/otomasi-industri/>

Direktorat Jenderal Pendidikan Vokasi. (2021). *Kebijakan Pendidikan Vokasi di Era Digital*. Kementerian Pendidikan, Kebudayaan, Riset, dan Teknologi.

Erizal, N. (2024). *AI dan otomatisasi ubah lanskap pekerjaan di Indonesia*. Kumparan

BM Security. (2022). *IBM X-Force Threat Intelligence Index 2022*.

Nexus Integra. (2023). *10 benefits of counting with an industrial automation system*.

SQURA Cybersecurity. (2024). *Apa itu cyber security & 5 kelebihannya yang wajib tahu*

Jurnal:

- Anaam, I. K., Hidayat, T., Pranata, R. Y., Abdillah, H., & Putra, A. Y. W. (2022). Pengaruh trend otomasi dalam dunia manufaktur dan industri. *Vocational Education National Seminar (VENS)*
- Anthony, A., Sedyono, E., & Iriani, A. (2020). Analisis kesiapan kerja mahasiswa di era Revolusi Industri 4.0 menggunakan Soft-System Methodology. *Jurnal Teknologi Informasi dan Ilmu Komputer*,
- Anwar, M. (2021). Literasi digital dalam dunia kerja era Revolusi Industri 4.0. *Jurnal Pendidikan Vokasi*
- Budi, E., Wira, D., & Infantono, A. (2021). Strategi penguatan cyber security guna mewujudkan keamanan nasional di era Society 5.0. *Prosiding Seminar Nasional Sains Teknologi dan Inovasi Indonesia*.
- Dwi Saputro, Y., & Nugroho, S. (2023). Aplikasi PLC Siemens S7-1200 untuk sistem kontrol dan monitoring. *Jurnal Teknik Elektro*
- Fajaruddin, M., & Wibowo, Y. (2021). Implementasi IIoT untuk pemeliharaan prediktif pada motor induksi. *Jurnal Teknik Industri*.
- Fauzi, M., & Lestari, Y. (2020). Peran IoT dalam mewujudkan konsep smart factory di era Industri 4.0. *Jurnal Teknik Komputer*.
- Fauziah, N., dkk. (2023). Analisis kebutuhan kompetensi cybersecurity pada kurikulum pendidikan vokasi era Industri 4.0. *Jurnal Pendidikan Teknik Elektro*.
- Handayani, R. (2022). Etos kerja dan tantangan tenaga kerja di era digital. *Jurnal Manajemen & Bisnis*, 9(1), 67–78.
- Handoko, E., & Purwanto, A. (2020). Perancangan sistem SCADA berbasis web untuk pengendalian level air. *Jurnal Teknik Elektro*.
- Hoshmand, M. O., & Ratnawati, S. (2023). Analisis keamanan infrastruktur teknologi informasi dalam menghadapi ancaman cybersecurity. *Jurnal Sains dan Teknologi*, 5(2), 679–686.
- Huzaifah, A. S. (2024). Peningkatan kompetensi mahasiswa di bidang network computer dan cyber security melalui program studi independen Merdeka Belajar Kampus Merdeka. *Jurnal Pengabdian Bersama Masyarakat Indonesia*, 2(3), 53–60.
- Kurniasari, F. B. (2022). Perkembangan programmable logic controller (PLC) di era Industri 4.0. *TATAL: Jurnal Teknik Industri dan Teknologi*, 2(1).
- Permana, R. A., Anindita, R., Zainol, Z., & Quinn, A. (2025). Analisis metode dan teknologi untuk perlindungan data dan informasi dari ancaman siber. *Jurnal MENTARI: Manajemen, Pendidikan dan Teknologi Informasi*, 3(2), 137–146.
- Purwadi, S., & Kholiq, A. (2023). Pengembangan HMI dengan desain high performance untuk efisiensi operasional. *Jurnal Otomasi Industri*.
- Rahmat, T., Ashshiddiqi, M. T., & Apriliani, D. (2024). Urgency of digital literacy to improving work readiness in the Industrial Revolution 4.0. *The Journal of Society and Media*, 8(1), 307–326.
<https://doi.org/10.26740/jsm.v8n1.p307-326>
- Ramadhani, A., & Susanto, W. (2024). Perancangan HMI multi-touch pada panel kontrol mesin produksi. *Jurnal Rekayasa Otomasi*.
- Riyandhika, R. R. (2020). Analisis kesadaran cybersecurity pada kalangan mahasiswa di Indonesia. *AUTOMATA*, 1(2).
- Rohman, M., Setiawan, R., & Lestari, A. (2022). Faktor-faktor yang memengaruhi kesiapan kerja siswa vokasi di Indonesia. *Jurnal Pendidikan Teknologi dan Kejuruan*, 28(3), 201–213.
- Setiadi, A., & Santoso, B. (2022).

- Integrasi PLC dalam arsitektur IIoT untuk smart manufacturing. Jurnal Sistem dan Teknologi Informasi.*
- Setiawan, D. (2022). Studi implementasi cloud-based SCADA untuk infrastruktur distribusi air. *Jurnal Sains dan Teknologi.*
- Suparno, S., Purwana, D., Wibowo, A., & Narmaditya, B. S. (2023). Industrial education 4.0: The role of human, technology, and data literacy. *Journal of Media Literacy Education*, 15(3), 27–40.
<https://doi.org/10.23860/JMLE-2023-15-3-3>
- Supriyanto, E. (2020). Peran soft skills dalam mendukung kompetensi kerja lulusan vokasi. *Jurnal Psikologi dan Pendidikan*, 14(1), 45–55.
- Suriadi. (2022). Keamanan sistem informasi dan serangan siber di Industri 4.0. *Jurnal Teknologi Informasi*, 5(1), 12–25.
- Telaumbanua, A., & Telaumbanua, A. (2024). Pengaruh soft skill dan hard skill mahasiswa terhadap kesiapan kerja di era Revolusi Industri 4.0. *Jurnal Suluh Pendidikan*, 12(2), 126–136.
- Wibowo, A. (2021). Penguasaan keterampilan teknis sebagai penentu kesiapan kerja lulusan SMK. *Jurnal Teknik dan Kejuruan*