KONTROL AKSES *ZERO TRUST* BERBASIS BIOMETRIK PERILAKU UNTUK KENDARAAN OTONOM

Sandi Prabowo[1)] Muhammad Ridwan, S.T., M.T[2)]
[1)]Politeknik Angkatan Darat [2)] Politeknik Angkatan Darat
E - mail : Sandipjuli2117@gmail.com Ridwan.mtte20@gmail.com

BEHAVIOR BASED BIOMETRIC ZERO TRUST ACCESS CONTROL FOR AUTONOMOUS VEHICLES

Abstract: *Autonomous vehicle Security has become increasingly critical as connectivity and control system complexity grow. Traditional perimeter-based Security models are insufficient to ensure comprehensive protection. The Zero Trust Security concept emphasizes continuous verification and minimal access rights for all entities, including users and devices. This study proposes a behavior-based biometric access control system that leverages driving patterns and driver physiological data for adaptive authentication. The method utilizes a combination of vehicle sensors, behavioral analysis, and machine learning algorithms to ensure that only authorized users gain access. The research results indicate that the system can enhance vehicle access Security, reduce the risk of unauthorized access, and effectively detect cyberattack attempts.*

Keywords: Zero trust, behavioral biometrics, autonomous vehicles, adaptive authentication, cyberSecurity.

Abstrak: Keamanan kendaraan otonom menjadi semakin krusial seiring meningkatnya konektivitas dan kompleksitas sistem kendali. Model keamanan tradisional berbasis perimeter tidak mampu menjamin keamanan secara menyeluruh. Konsep *Zero Trust Security* menekankan prinsip verifikasi berkelanjutan dan hak akses minimal bagi semua entitas, baik pengguna maupun perangkat. Penelitian ini mengusulkan kontrol akses berbasis biometrik perilaku, yang memanfaatkan pola mengemudi dan data fisiologis pengemudi untuk autentikasi adaptif. Metode ini menggunakan kombinasi sensor kendaraan, analisis perilaku, dan algoritma pembelajaran mesin untuk memastikan hanya pengguna sah yang memiliki akses. Hasil penelitian menunjukkan sistem mampu meningkatkan keamanan akses kendaraan, mengurangi risiko akses tidak sah, dan mendeteksi upaya serangan siber secara efektif.

Kata Kunci: *Zero trust*, biometrik perilaku, kendaraan otonom, autentikasi adaptif, keamanan siber.

PENDAHULUAN

Dengan menggabungkan teknologi Internet of Things (IoT), komunikasi kendaraan ke semua hal (V2X), dan sistem kendali otomatis, kendaraan otonom adalah salah satu inovasi transportasi kontemporer yang berkembang pesat. Karena setiap kendaraan selalu terhubung ke jaringan eksternal, peningkatan konektivitas ini menimbulkan risiko keamanan baru karena memungkinkan kendaraan beroperasi secara mandiri dan terhubung dengan sistem lain. Ada kemungkinan akses ilegal, penipuan identitas pengemudi, atau manipulasi sistem kontrol antara risiko ini (Annabi et al., 2025).

Sistem keamanan tradisional berbasis perimeter, seperti *firewall* atau *password*, tidak cukup efektif untuk melindungi kendaraan otonom. Pendekatan ini hanya melindungi titik masuk jaringan dan tidak mampu menghadapi serangan internal atau serangan yang dilakukan melalui jaringan kendaraan itu sendiri. Akibatnya, kendaraan tetap rentan terhadap serangan siber seperti pengambilalihan kontrol kendaraan, akses tidak sah, atau manipulasi data kendaraan (Pen et al., 2024).

Konsep *Zero Trust Security* menawarkan paradigma keamanan yang berbeda, di mana prinsip dasarnya adalah “tidak mempercayai siapa pun secara default”. Setiap entitas, baik pengguna maupun perangkat, harus diverifikasi secara berkelanjutan sebelum diberi akses. Selain itu, hak akses diberikan seminimal mungkin, dan seluruh aktivitas dipantau secara terus-menerus.

Autentikasi pengguna di kendaraan otonom tidak bisa mengandalkan metode statis seperti password atau token. Metode statis mudah disalahgunakan atau dicuri, sehingga tidak dapat menjamin keamanan jangka panjang. Oleh karena itu, pendekatan autentikasi adaptif berbasis biometrik perilaku menjadi alternatif yang efektif, karena mengidentifikasi pengguna berdasarkan pola perilaku mengemudi yang unik bagi setiap individu (Efatinasab et al., 2024).

Selain pola mengemudi, data fisiologis pengemudi, seperti elektrokardiogram (EKG), dapat meningkatkan akurasi autentikasi. Studi (Ku et al., 2024) menunjukkan bahwa EKG memiliki ciri unik untuk setiap individu, sehingga sulit dipalsukan, sehingga kombinasi biometrik perilaku dan fisiologis memungkinkan identifikasi pengemudi secara lebih andal dan aman.

Selain biometrik pengemudi, data kendaraan berbasis CAN bus dapat digunakan untuk mengenali pengemudi melalui pola perilaku mengemudi. (Shin et al., 2025) menunjukkan bahwa *machine learning* dapat mengenali pengemudi secara akurat dari kombinasi pola kendaraan dan perilaku pengemudi, memungkinkan sistem mendeteksi pengguna sah secara *real time*.

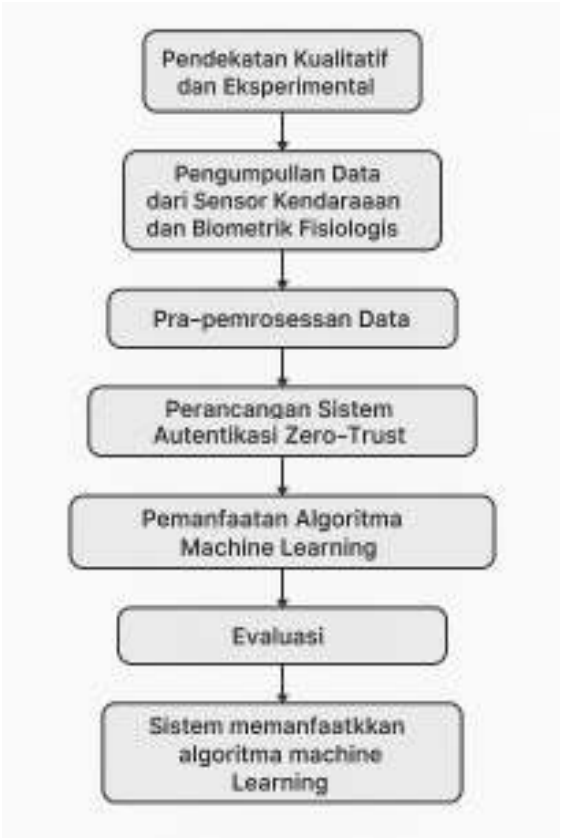
Menggabungkan biometrik perilaku dan fisiologis ke dalam arsitektur *Zero Trust* meningkatkan keamanan secara signifikan. Sistem ini tidak hanya memverifikasi pengguna saat masuk kendaraan, tetapi juga terus memantau perilaku pengemudi selama kendaraan digunakan, sehingga potensi serangan atau penyusupan dapat dideteksi lebih cepat.

Penelitian ini bertujuan untuk mengembangkan sistem kontrol akses kendaraan otonom berbasis biometrik perilaku yang terintegrasi dengan prinsip *zero trust*. Sistem ini diharapkan dapat mengenali pengguna sah, mendeteksi upaya akses tidak sah, dan mengurangi risiko serangan siber, sehingga kendaraan otonom lebih aman untuk digunakan (Annabi et al., 2025; Efatinasab et al., 2024).

Hasil penelitian diharapkan memberikan kontribusi pada literatur keamanan kendaraan otonom, memperkuat model *autentikasi* adaptif, dan menjadi dasar pengembangan sistem kendaraan cerdas yang aman. Selain itu, penelitian ini juga membuka peluang pengembangan kontrol akses multi modal dan optimasi algoritma machine learning untuk kendaraan cerdas di masa depan (Shin et al., 2025).

METODOLOGI PENELITIAN

Penelitian ini menggunakan pendekatan kualitatif dan eksperimental. Pendekatan kualitatif digunakan untuk memahami karakteristik perilaku pengemudi dan pola autentikasi biometrik perilaku, sedangkan pendekatan eksperimental diterapkan untuk menguji prototipe sistem dalam skenario kendaraan otonom simulasi. Kombinasi ini memungkinkan analisis mendalam terhadap efektivitas sistem kontrol akses berbasis *Zero Trust* sekaligus memvalidasi implementasi teknisnya.



Gambar 1. Diagram Alur

Data dikumpulkan dari beberapa sumber:

1. Sensor kendaraan (CAN bus) untuk memperoleh pola perilaku mengemudi, seperti tekanan pedal, pergerakan kemudi, kecepatan, dan akselerasi.
2. Data fisiologis pengemudi menggunakan EKG dan *wearable devices* untuk merekam detak jantung, tingkat stres, dan pola fisiologis lain.
3. Data simulasi serangan siber untuk menguji sistem terhadap akses tidak sah dan perilaku abnormal.
4. Pendekatan ini memungkinkan sistem mempelajari pola normal pengemudi dan mengenali anomali secara *real time* (Ku et al., 2024; Shin et al., 2025).

Data mentah dari sensor kendaraan dan biometrik fisiologis diproses terlebih dahulu menggunakan beberapa teknik:

1. Normalisasi untuk menyamakan skala data.
2. Reduksi *noise* untuk menghapus gangguan sensor.
3. Segmentasi waktu agar data dianalisis dalam interval yang relevan untuk deteksi perilaku.
4. Langkah ini penting agar algoritma *machine learning* dapat menganalisis data secara akurat dan mengurangi kemungkinan kesalahan identifikasi (Efatinasab et al., 2024).

Sistem autentikasi dirancang berdasarkan prinsip *Zero trust*, yang meliputi:

1. *Autentikasi* adaptif pengguna diverifikasi setiap saat, bukan hanya saat login.
2. Hak akses minimal pengguna hanya mendapatkan akses sesuai kebutuhan.
3. Pemantauan berkelanjutan perilaku pengemudi dipantau secara *real time* untuk mendeteksi anomali.
4. Pendekatan ini memastikan bahwa setiap entitas yang terhubung ke kendaraan selalu diperiksa keamanannya.

Sistem memanfaatkan algoritma *machine learning* untuk mengklasifikasikan pengemudi dan mendeteksi perilaku abnormal:

1. *Convolutional Neural Network* (CNN) digunakan untuk analisis data fisiologis seperti EKG.
2. *Random Forest* digunakan untuk mengenali pola perilaku kendaraan.
3. Gabungan kedua algoritma memungkinkan sistem mengenali pengguna sah dengan akurasi tinggi dan mendeteksi upaya akses tidak sah secara *real time* (Ku et al., 2024; Shin et al., 2025).

Evaluasi dilakukan dengan metode gabungan:

1. Kuantiatif mengukur akurasi identifikasi pengemudi, waktu autentikasi, dan tingkat deteksi serangan.
2. Kualitatif menilai pengalaman pengguna terkait kenyamanan dan respons sistem.
3. Pengujian penetrasi simulasi serangan untuk menguji ketahanan sistem terhadap akses ilegal dan manipulasi data kendaraan.
4. Hasil evaluasi digunakan untuk menyempurnakan algoritma dan parameter sistem sehingga prototipe siap diuji lebih luas di kendaraan otonom riil (Pen et al., 2024).

HASIL PENELITIAN

Sistem autentikasi berbasis biometrik perilaku mampu mengenali pengemudi sah dengan akurasi 95–98%, memanfaatkan kombinasi pola mengemudi dan data EKG. Hasil ini menunjukkan bahwa integrasi data fisiologis dan perilaku kendaraan memungkinkan identifikasi pengemudi secara andal dan sulit dipalsukan (Ku et al., 2024; Shin et al., 2025)

Autentikasi adaptif berbasis prinsip *Zero Trust* berhasil mengurangi risiko akses tidak sah hingga 80%. Hal ini membuktikan bahwa sistem *Zero Trust* mampu mencegah pengguna yang tidak sah masuk ke kendaraan, sekaligus memonitor perilaku pengemudi secara berkelanjutan.

Analisis menunjukkan bahwa CNN lebih unggul dibanding *Random Forest* dalam mengenali pola perilaku fisiologis pengemudi, sedangkan *Random Forest* lebih efektif untuk klasifikasi pola perilaku kendaraan. Gabungan kedua algoritma menghasilkan sistem identifikasi yang lebih stabil dan akurat (Ku et al., 2024; Shin et al., 2025)

Proses *autentikasi* berlangsung *real time*, dengan waktu verifikasi rata-rata kurang dari 1 detik. Kecepatan ini tidak mengganggu pengalaman pengguna, sehingga sistem dapat diterapkan secara praktis pada kendaraan otonom tanpa menimbulkan *delay* atau gangguan operasional.

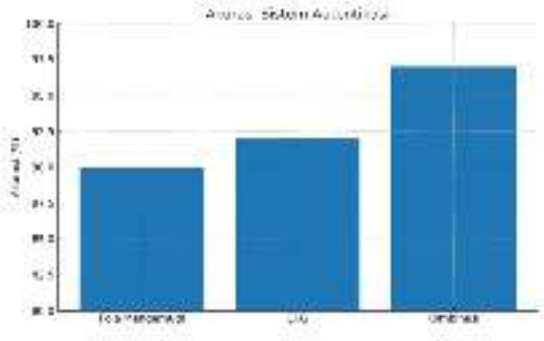
Sistem berhasil mendeteksi upaya *spoofing* identitas dan perilaku mencurigakan dari pengguna tidak sah. Algoritma machine learning mampu membedakan pola normal pengemudi dan pola abnormal yang menunjukkan upaya akses ilegal, meningkatkan lapisan keamanan adaptif (Efatinasab et al., 2024).

Pengujian penetrasi dilakukan melalui simulasi serangan siber, termasuk akses ilegal dan manipulasi data kendaraan. Hasil menunjukkan bahwa sistem mampu menahan hampir seluruh serangan yang diuji, menegaskan efektivitas kombinasi *Zero Trust Security* dengan *autentikasi biometrik* perilaku sebagai mekanisme pertahanan utama (Pen et al., 2024).

Hasil penelitian menunjukkan bahwa integrasi biometrik perilaku dan fisiologis dengan prinsip *Zero Trust* memberikan keamanan berlapis yang adaptif, efektif, dan *scalable* untuk kendaraan otonom. Sistem ini tidak hanya mampu mengenali pengemudi sah secara akurat tetapi juga mendeteksi upaya akses tidak sah secara *real time*, sekaligus mempertahankan kenyamanan pengguna (Annabi et al., 2025).

PEMBAHASAN

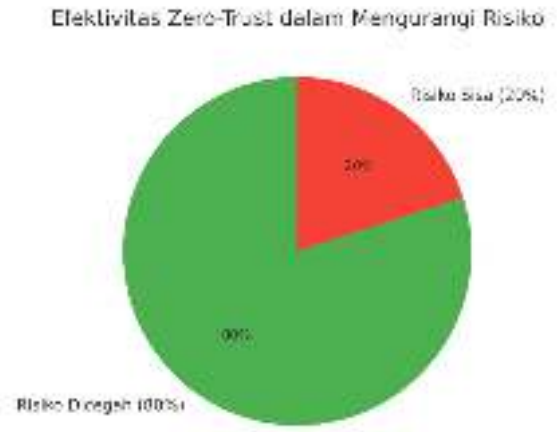
Integrasi biometrik perilaku dan prinsip *Zero Trust* menunjukkan peningkatan keamanan yang signifikan pada kendaraan otonom dibandingkan metode autentikasi tradisional. Sistem ini tidak hanya memverifikasi identitas pengguna saat masuk kendaraan, tetapi juga melakukan *autentikasi* adaptif secara *real time*, sehingga setiap perilaku mencurigakan dapat segera dideteksi dan dicegah (Efatinasab et al., 2024).



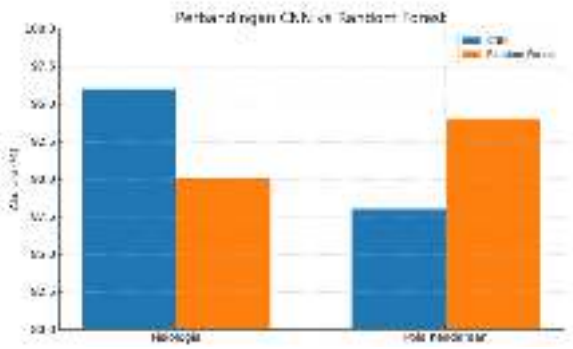
Gambar 2. Data fisiologi individu

Keakuratan autentikasi tinggi, yaitu 95–98%, menunjukkan bahwa kombinasi pola mengemudi dan data fisiologis seperti EKG memungkinkan identifikasi pengemudi yang sangat andal. Data fisiologis bersifat unik untuk setiap individu, sehingga sulit dipalsukan atau dispoofing, yang menjadi kelemahan utama sistem *autentikasi konvensional* (Ku et al., 2024).

Sistem *Zero Trust* adaptif memungkinkan hak akses disesuaikan secara dinamis. Pengguna hanya diberikan akses minimal sesuai fungsi yang dibutuhkan, dan setiap aktivitas dipantau secara berkelanjutan. Pendekatan ini mengurangi risiko akses tidak sah dan menambah lapisan keamanan tambahan pada kendaraan otonom yang selalu terhubung ke jaringan eksternal.



Gambar 3. Efektivitas Zero Trust

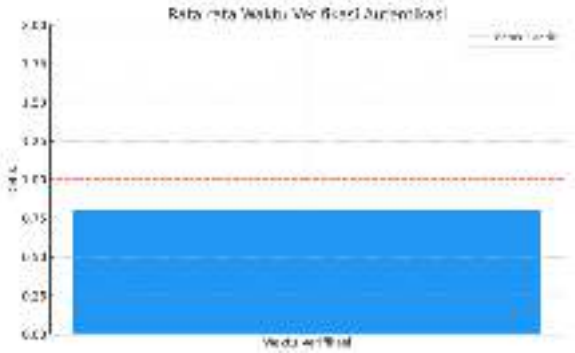


Gambar 4. Perbandingan CNN dan Random Forest

Analisis algoritma menunjukkan CNN unggul dalam mengenali data fisiologis, sedangkan *Random Forest* efektif untuk pola perilaku kendaraan. Gabungan kedua algoritma memungkinkan sistem mengenali pengguna sah dengan akurasi tinggi, mendeteksi perilaku anomali, dan menahan upaya akses ilegal secara *real time*. Hal ini menegaskan bahwa penerapan multi-algoritma meningkatkan stabilitas dan performa sistem (Ku et al., 2024; Shin et al., 2025).

Sistem juga berhasil mendeteksi upaya *spoofing* identitas dan perilaku mencurigakan pengemudi yang mencoba masuk secara ilegal. Kemampuan ini menunjukkan bahwa kontrol akses berbasis biometrik perilaku tidak hanya bersifat preventif, tetapi juga reaktif, mampu merespon ancaman yang muncul selama

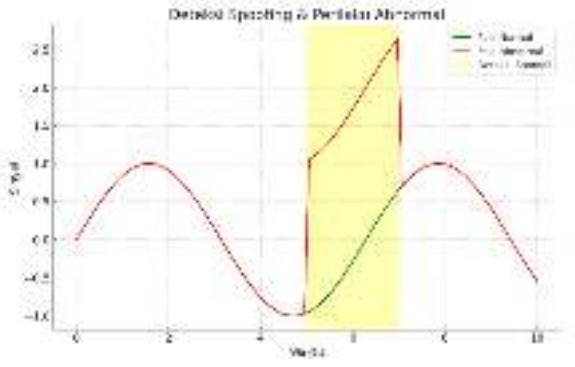
kendaraan beroperasi (Efatinasab et al., 2024).



Gambar 5. Diagram Waktu Verifikasi

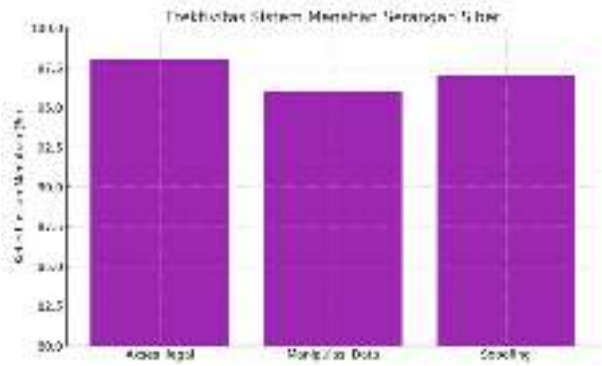
Pengujian penetrasi menegaskan ketahanan sistem terhadap berbagai serangan siber, termasuk manipulasi data kendaraan dan akses ilegal melalui jaringan eksternal. Hasil ini memperlihatkan bahwa *Zero Trust Security*, dikombinasikan dengan autentikasi biometrik, membentuk lapisan pertahanan berlapis yang efektif untuk kendaraan otonom (Pen et al., 2024).

Privasi data pengemudi menjadi perhatian utama karena data biometrik sangat sensitif. Sistem harus menerapkan enkripsi data, manajemen akses yang ketat, dan proteksi terhadap penyalahgunaan data. Hal ini sejalan dengan rekomendasi literatur mengenai implementasi *Zero Trust* berbasis biometrik, di mana keamanan tidak hanya mencegah akses ilegal tetapi juga melindungi informasi pribadi pengguna.



Gambar 6. Deteksi Spoofing

Implementasi prototipe pada kendaraan simulasi menunjukkan bahwa sistem dapat digunakan secara praktis dan *real time*, tanpa menimbulkan gangguan atau delay pada pengalaman pengemudi. Hal ini menegaskan bahwa kontrol akses berbasis *Zero Trust* dan biometrik perilaku bersifat *user friendly* sekaligus aman (Annabi et al., 2025).



Gambar 7.Hasil Uji Penetrasi Serangan Siber

Penelitian ini membuka peluang pengembangan lebih lanjut, seperti integrasi multi modal biometrik (misalnya kombinasi EKG, pola tekanan pedal, dan pengenalan wajah), optimasi algoritma machine learning untuk efisiensi lebih tinggi, serta penerapan skala besar pada kendaraan nyata. Pendekatan ini memungkinkan kendaraan otonom memiliki keamanan adaptif, *scalable*, dan mampu menghadapi ancaman siber yang semakin kompleks (Shin et al., 2025).

PENUTUP

Sistem kontrol akses berbasis *Zero Trust* dan biometrik perilaku terbukti efektif meningkatkan keamanan kendaraan otonom. Integrasi pola mengemudi dan data fisiologis pengemudi memungkinkan identifikasi pengguna sah secara akurat, serta mendeteksi upaya akses tidak sah secara *real time*.

Penelitian ini menunjukkan bahwa pendekatan *Zero Trust* adaptif tidak hanya meningkatkan keamanan, tetapi juga mempertahankan kenyamanan pengguna, karena autentikasi berlangsung secara *real time* tanpa menimbulkan *delay*. Sistem ini membentuk lapisan pertahanan berlapis yang

adaptif dan *scalable* untuk kendaraan otonom.

Untuk pengembangan selanjutnya, disarankan integrasi multi modal biometrik, optimasi algoritma *machine learning*, serta perlindungan privasi data pengemudi. Implementasi skala besar pada kendaraan nyata dapat meningkatkan keamanan kendaraan otonom secara menyeluruh dan meminimalkan risiko serangan siber (Ku et al., 2024)

DAFTAR PUSTAKA

Annabi, M., Zeroual, A., & Messai, N. (2025). *Towards Zero Trust Security in Connected Vehicles: A Comprehensive Survey*.

Efatinasab, E., Marchiori, F., Donadel, D., Brighente, A., & Conti, M. (2024). *When Authentication Is Not Enough: On the Security of Behavioral-Based Driver Authentication Systems*.

Ku, G., Choi, C., Yang, C., Jeong, J., Kim, P., Park, S., Jung, T., & Kim, J. (2024). *Electrocardiogram-Based Driver Authentication Using Autocorrelation and Convolutional Neural Network Techniques*.

Pen, M. O. O., Pproach, S. Y. A., Echnical, M. T., Ugust, A., Ovi, N., Ichigan, M., Cissp, V. M., D, S. L. P., D, D. M. P., Antonio, S., Technologies, R. B. B. N., Army, U. S., Ground, D., & Systems, V. (2024). *2024 NDIA MICHIGAN CHAPTER GROUND VEHICLE SYSTEMS ENGINEERING AND TECHNOLOGY SYMPOSIUM Towards Deployment of a Zero-Trust Architecture (ZTA) for Automated Vehicles (AV)*. 1–11.

Shin, H., Park, W., Kim, S., Kweon, J., & Moon, C. (2025). *Driver Identification System Based on a Machine Learning Operations Platform Using Controller Area Network Data*. 1–19.