Jurnal Ilmiah Ilmu Komputer & Elektronika (MURAKOM)
Volume. 2 Nomor. 3 Juli 2026
e-ISSN : 3123-1985; p-ISSN : 3110-4754, Hal. 100-110
DOI: https://doi.org/10.64365/murakom.v2i3.473
Available online at: *https://jurnal.muaraedukasi.id/index.php/murakom*

Kerangka Keamanan untuk Gardu Digital dan Infrastruktur Energi Terdistribusi

Hendra Wijaya Kusuma [1*],Indah Permata Sari [2]
[1,2] Universitas Gunadarma, Indonesia
Alamat: Jl. Margonda Raya No. 100, Pondok Cina, Kec. Beji, Kota Depok, Jawa Barat.
Email : hendrawijayauksuma@gunadarma.ac.id [1*], indahpermatasari@gunadarma.ac.id [2]
Korespondensi penulis : hendrawijayauksuma@gunadarma.ac.id

Abstract*. The digital transformation of electric power systems, particularly through the deployment of digital substations and distributed energy resources (DER), has significantly improved operational efficiency and flexibility. However, the convergence of operational technology (OT) and information technology (IT) has also expanded the cyber-attack surface, making digital substations and DER prime targets for cyber threats that could disrupt national grid stability. This study aims to design and propose a comprehensive security framework that is adaptive to the unique characteristics of digital substations (based on IEC 61850) and the dynamic nature of distributed energy resources such as solar panels, battery storage, and microgrids. The developed framework integrates zero trust architecture principles, machine learning-based anomaly detection, and lightweight encryption protocols to address computational resource constraints on edge devices. The methodology includes threat modeling based on the NIST IR 8228 framework and cyber-attack simulations (e.g., man-in-the-middle and denial-of-service) within a hybrid testbed environment. The results show that the proposed framework can detect 97.2% of cyber-attacks with an average detection latency below 200 milliseconds, while mitigating the risk of cascading failures in distributed systems. The main contribution of this research is the provision of technical guidelines for distribution system operators and energy stakeholders to enhance the cyber resilience of digital substations without compromising real-time performance.*

Keywords: *digital substation, distributed energy infrastructure, cyber security, zero trust, anomaly detection, IEC 61850.*

Abstrak. Transformasi digital pada sistem tenaga listrik, terutama melalui implementasi gardu digital dan integrasi infrastruktur energi terdistribusi (Distributed Energy Resources/DER), telah meningkatkan efisiensi dan fleksibilitas operasional. Namun, konvergensi antara teknologi operasional (OT) dan teknologi informasi (IT) juga memperluas permukaan serangan siber, menjadikan gardu digital dan DER sebagai target potensial bagi ancaman siber yang dapat mengganggu stabilitas jaringan nasional. Penelitian ini bertujuan untuk merancang dan mengusulkan kerangka keamanan komprehensif yang adaptif terhadap karakteristik unik gardu digital (berbasis IEC 61850) dan sifat dinamis dari energi terdistribusi seperti panel surya, penyimpanan baterai, dan mikrogrid. Kerangka yang dikembangkan mengintegrasikan prinsip zero trust architecture, deteksi anomali berbasis machine learning, serta protokol enkripsi ringan untuk mengatasi keterbatasan sumber daya komputasi pada perangkat tepi (edge devices). Metodologi yang digunakan mencakup pemodelan ancaman berbasis standar NIST IR 8228 dan simulasi serangan siber (seperti man-in-the-middle dan denial-of-service) pada lingkungan uji hybrid. Hasil penelitian menunjukkan bahwa kerangka yang diusulkan mampu mendeteksi 97,2% serangan siber dengan latensi deteksi rata-rata di bawah 200 milidetik, serta memitigasi risiko kegagalan berantai pada sistem terdistribusi. Kontribusi utama dari penelitian ini adalah tersedianya panduan teknis bagi operator sistem distribusi dan pemangku kepentingan energi dalam memperkuat ketahanan siber gardu digital tanpa mengorbankan kinerja real-time.

Kata Kunci: gardu digital, infrastruktur energi terdistribusi, keamanan siber, zero trust, deteksi anomali, IEC 61850.

1. LATAR BELAKANG

Transisi menuju sistem energi modern ditandai dengan integrasi masif teknologi digital dan sumber energi terbarukan. Gardu konvensional yang berbasis perangkat analog dan kabel tembaga secara bertahap digantikan oleh gardu digital yang memanfaatkan protokol

Received: April 28, 2026; Revised: Mei 12, 2026; Accepted: Mei 30, 2026; Online Available: Juni 15, 2026; Published: Juli 13,2026

komunikasi digital seperti IEC 61850 dan proses bus berbasis ethernet. Paralel dengan itu, infrastruktur energi terdistribusi (Distributed Energy Resources/DER) seperti panel surya atap, turbin angin skala kecil, dan sistem penyimpanan energi baterai semakin banyak terhubung ke jaringan distribusi.

Namun, transformasi ini membawa konsekuensi serius terhadap aspek keamanan. Gardu digital dan DER sangat bergantung pada konektivitas jaringan dan sistem pemantauan jarak jauh, yang secara inheren rentan terhadap serangan siber. Beberapa insiden dunia nyata, seperti serangan terhadap jaringan listrik Ukraina (2015 & 2016) dan insiden ransomware pada infrastruktur kritis AS (Colonial Pipeline 2021), menunjukkan bahwa sektor energi adalah target utama pelaku ancaman.

Terdapat beberapa tantangan utama yang melatarbelakangi perlunya kerangka keamanan khusus:

a. Perbedaan Karakteristik OT dan IT: Sistem kontrol industri (ICS) di gardu digital memiliki persyaratan real-time, ketersediaan tinggi, dan umur perangkat yang panjang, sehingga pendekatan keamanan siber konvensional yang dirancang untuk IT sering kali tidak cocok atau bahkan membahayakan operasi.
b. Kompleksitas dan Skalabilitas: Jumlah DER yang terus bertambah secara eksponensial (bersifat heterogen dan tersebar secara geografis) menciptakan permukaan serangan yang sangat luas. Mekanisme keamanan terpusat tidak lagi efisien.
c. Keterbatasan Sumber Daya: Banyak perangkat tepi (edge devices) pada gardu digital dan DER memiliki daya komputasi dan memori terbatas, sehingga tidak mampu menjalankan solusi keamanan berat seperti enkripsi asimetris penuh atau antivirus berbasis host.
d. Standar yang Belum Matang: Meskipun standar seperti IEC 62351 menyediakan panduan keamanan untuk protokol IEC 61850, implementasinya masih parsial dan belum secara khusus mengatasi sifat dinamis dari infrastruktur energi terdistribusi.

Berdasarkan latar belakang tersebut, penelitian ini dirancang untuk mengembangkan kerangka keamanan yang terintegrasi, adaptif, dan ringan. Kerangka ini diharapkan mampu melindungi gardu digital dan DER dari ancaman siber modern (termasuk zero-day attack dan serangan supply chain) tanpa mengorbankan kinerja real-time yang menjadi tulang punggung keandalan sistem tenaga listrik.

2. KAJIAN TEORITIS

2.1 Kajian Teoritis

Kajian teoritis ini membahas landasan konseptual dan teori-teori yang menjadi dasar pengembangan kerangka keamanan untuk gardu digital dan infrastruktur energi terdistribusi (Distributed Energy Resources/DER). Teori-teori yang relevan dikelompokkan menjadi empat pilar utama: (1) arsitektur gardu digital, (2) infrastruktur energi terdistribusi, (3) ancaman dan kerentanan siber pada sistem tenaga, serta (4) model dan pendekatan keamanan siber.

2.11. Teori Gardu Digital (Digital Substation)

Gardu digital adalah gardu listrik yang menggunakan komunikasi digital serial (berbasis protokol IEC 61850) untuk menggantikan kabel tembaga konvensional. Menurut standar IEC 61850, arsitektur gardu digital terdiri dari tiga tingkatan utama:

a. Process Level: Berisi perangkat lapangan seperti transformator instrumen digital (*current/voltage transformer*), sensor cerdas, dan aktuator.
b. Bay Level: Berisi Intelligent Electronic Devices (IED) yang bertanggung jawab untuk proteksi, pengukuran, dan kontrol.
c. Station Level: Berisi sistem pengawasan (SCADA/HMI), gateway komunikasi, dan server engineering.

Teori komunikasi pada gardu digital menggunakan prinsip Generic Object Oriented Substation Events (GOOSE) untuk pesan cepat antar IED, dan Sampled Measured Values (SMV) untuk data pengukuran real-time. Kedua protokol ini berjalan pada jaringan ethernet dan tidak memiliki mekanisme keamanan bawaan (inherently insecure), sehingga menjadi celah utama serangan siber.

2.2 Teori Infrastruktur Energi Terdistribusi (DER)

Distributed Energy Resources (DER) mengacu pada sumber daya energi yang terhubung pada jaringan distribusi, bukan pada transmisi. Menangkap definisi dari U.S. Department of Energy (DOE) dan IEEE Std 1547-2018, DER mencakup:

a. Pembangkit terdistribusi (*distributed generation/DG*): panel surya, turbin angin, mikrohidro, fuel cell, genset.
b. Sistem penyimpanan energi (*battery energy storage system/BESS*).
c. Sistem respons permintaan (demand response) dan kendali beban.

Karakteristik utama DER adalah: (a) kapasitas kecil hingga menengah, (b) tersebar secara geografis, (c) bersifat intermiten (khususnya energi terbarukan), dan (d) sering dikelola secara agregat melalui virtual power plant (VPP). Teori keamanan DER harus mempertimbangkan

aspek grid-edge, di mana perangkat sering ditempatkan di lokasi publik atau tidak terjaga, sehingga rentan terhadap akses fisik tidak sah.

3. METODE PENELITIAN

3.1. Studi Literatur dan Analisis Kebutuhan

Tujuan: Mengidentifikasi state-of-the-art keamanan gardu digital dan DER, serta kesenjangan penelitian (*research gap*).

Langkah-langkah:

a. Mengumpulkan dan mensintesis literatur dari sumber terpercaya: IEEE Xplore, ScienceDirect, Scopus, serta standar internasional (IEC 61850, IEC 62351, IEC 62443, NIST SP 800-82, IEEE 1547).
b. Melakukan analisis kebutuhan keamanan spesifik untuk gardu digital (latensi < 4 ms untuk GOOSE, ketersediaan 99.999%) dan DER (sumber daya terbatas, konektivitas nirkabel).
c. Mengidentifikasi skenario serangan yang paling umum dan dampaknya terhadap stabilitas sistem tenaga.
d. Output: Daftar persyaratan fungsional dan non-fungsional kerangka keamanan.

3.2. Pemodelan Ancaman (Threat Modeling)

Tujuan: Memetakan secara sistematis aset, vektor serangan, dan potensi ancaman pada arsitektur gardu digital dan DER.

Metode yang digunakan: STRIDE (*Spoofing, Tampering, Repudiation, Information Disclosure, Denial of Service, Elevation of Privilege*) dan DREAD (*Damage, Reproducibility, Exploitability, Affected Users, Discoverability*) yang diadaptasi untuk lingkungan OT.

Langkah-langkah:

a. Menggambar diagram aliran data (*Data Flow Diagram/DFD*) untuk arsitektur referensi gardu digital (*process level, bay level, station level*) dan sistem DER (*inverter, aggregator, cloud platform*).
b. Mengidentifikasi aset kritis: IED, relay proteksi, RTU, smart meter, gateway komunikasi, SCADA server.
c. Untuk setiap aset, identifikasi ancaman potensial menggunakan matriks STRIDE.
d. Menentukan tingkat risiko menggunakan pendekatan kualitatif (rendah-sedang-tinggi) berdasarkan probabilitas dan dampak.

Output: Peta ancaman (*threat landscape*) dan prioritas risiko untuk setiap komponen.

3.3. Perancangan Kerangka Keamanan

Tujuan: Merancang arsitektur kerangka keamanan yang terintegrasi dan memenuhi persyaratan dari tahap 1 dan 2.

Langkah-langkah:

a. Perancangan Arsitektur Logis

1) Mengadopsi model zones and conduits dari IEC 62443.
2) Menentukan zona keamanan: Zona 1 (process level), Zona 2 (bay level), Zona 3 (station level), Zona 4 (DER edge), Zona 5 (cloud/aggregator).
3) Mendefinisikan conduit (saluran komunikasi) antar zona dengan kebijakan keamanan yang berbeda.

Tabel 1 Perancangan Komponen Keamanan

Komponen	Fungsi	Teknologi yang Digunakan
Autentikasi mutual	Mencegah spoofing dan MitM	Sertifikat digital X.509 dengan validasi waktu singkat (short-lived certificates)
Enkripsi ringan	Melindungi kerahasiaan data	AES-128-GCM untuk GOOSE/SMV; DTLS untuk komunikasi DER
Deteksi anomali	Mendeteksi serangan FDI, replay, DoS	Ensemble model: Isolation Forest + LSTM Autoencoder
Micro-segmentation	Membatasi lateral movement	VLAN dan firewall industri dengan deep packet inspection (DPI)
Incident response	Mitigasi otomatis	Rule engine: memblokir IED yang mencurigakan, beralih ke mode islanding aman

4. HASIL DAN PEMBAHASAN

4.1. Hasil Pengujian Kinerja Deteksi Serangan

4.1.1 Skenario Normal (*Baseline*)

Pada skenario tanpa serangan (S1), kerangka keamanan beroperasi dalam kondisi normal selama 30 menit pengamatan. Ditemukan bahwa false positive rate (FPR) sistem berada pada angka 2,1 persen. Artinya, dari seluruh lalu lintas jaringan normal yang dianalisis, sekitar 2,1 persen di antaranya salah terdeteksi sebagai anomali. Nilai FPR ini tergolong rendah dan masih berada dalam batas toleransi untuk sistem OT (operational technology) di mana alarm palsu

yang terlalu sering dapat menyebabkan kelelahan operator. Sebagian besar false positive berasal dari fluktuasi normal data Sampled Measured Values (SMV) pada saat perubahan beban mendadak dan dari pesan GOOSE yang sah namun memiliki pola waktu yang tidak biasa karena proses switching rutin.

4.1.2 Skenario Denial of Service (DoS)

Pada skenario S2, serangan DoS berupa SYN flood diluncurkan ke switch pada process level dengan kecepatan 1000 paket per detik. Kerangka keamanan berhasil mendeteksi serangan dengan true positive rate (TPR) sebesar 96,4 persen dan FPR sebesar 3,2 persen. Waktu deteksi rata-rata tercatat 145 milidetik dengan standar deviasi 23 milidetik, sementara waktu mitigasi (tindakan otomatis memblokir alamat IP sumber) memerlukan 0,87 detik. Hasil ini menunjukkan bahwa deteksi anomali berbasis Isolation Forest mampu mengenali pola lonjakan paket yang tidak normal dengan cukup cepat. Namun, sekitar 3,6 persen serangan DoS tidak terdeteksi karena volume serangan yang masih berada di bawah ambang batas anomali atau karena pola serangan yang menyerupai lalu lintas broadcast normal pada jaringan IEC 61850.

4.1.3 Skenario Man-in-the-Middle (MitM)

Pada skenario S3, serangan MitM melalui ARP spoofing dilakukan antara IED pengukuran dan relay proteksi. Kerangka keamanan menunjukkan kinerja terbaik untuk skenario ini dengan TPR mencapai 98,1 persen dan FPR hanya 1,8 persen. Detection latency tercatat 98 milidetik (rata-rata) dan waktu mitigasi 0,52 detik. Keberhasilan deteksi yang tinggi ini disebabkan oleh implementasi mekanisme autentikasi mutual berbasis sertifikat digital X.509 dengan masa berlaku pendek. Setiap pesan GOOSE dan MMS dilengkapi dengan tanda tangan digital, sehingga percobaan penyadapan atau modifikasi pesan oleh pihak ketiga langsung terdeteksi karena ketidaksesuaian tanda tangan. Serangan MitM yang berhasil lolos deteksi (sekitar 1,9 persen) terjadi pada saat pergantian sertifikat di mana ada celah singkat sebelum sertifikat baru terdistribusi ke semua IED.

4.2 Pembahasan

4.2.1 Efektivitas Deteksi Anomali Berbasis Ensemble

Hasil pengujian menunjukkan bahwa kombinasi Isolation Forest dan LSTM Autoencoder memberikan kinerja deteksi yang baik dengan TPR rata-rata di atas 96 persen. Isolation Forest terbukti efektif untuk deteksi cepat serangan berbasis anomali statistik seperti DoS dan FDI dengan perubahan nilai yang drastis. Sementara itu, LSTM Autoencoder lebih unggul dalam menangkap anomali pola temporal yang halus, seperti replay attack dan FDI dengan slow drift. Pendekatan ensemble ini mengatasi kelemahan masing-masing algoritma jika digunakan secara terpisah. Namun, pada serangan kombinasi (S6), terjadi kompetisi sumber daya komputasi

antara kedua model yang menyebabkan peningkatan latensi dan sedikit penurunan akurasi. Untuk penelitian selanjutnya, disarankan untuk menerapkan mekanisme prioritas dinamis di mana model yang lebih ringan (Isolation Forest) dipanggil terlebih dahulu, dan LSTM Autoencoder hanya diaktifkan jika diperlukan konfirmasi lebih lanjut.

4.2.2 Keunggulan Zero Trust pada Lingkungan OT

Implementasi prinsip zero trust melalui autentikasi mutual dan micro-segmentation terbukti efektif dalam memblokir serangan MitM dan membatasi lateral movement. Pendekatan ini berbeda secara fundamental dengan model keamanan tradisional yang mengandalkan perimeter defense. Dalam pengujian, ketika satu IED berhasil dikompromikan pada skenario compound attack, micro-segmentation mencegah penyerang mengakses IED lain di zona yang berbeda. Hal ini sangat penting mengingat gardu digital memiliki banyak IED yang saling terhubung. Tantangan utama dalam menerapkan zero trust pada OT adalah manajemen siklus hidup sertifikat digital. Pergantian sertifikat yang terlalu sering (untuk meningkatkan keamanan) berisiko menciptakan celah waktu di mana autentikasi belum diperbarui secara seragam di seluruh perangkat.

4.2.3 Kompromi antara Keamanan dan Kinerja Real-Time

Temuan penting dari penelitian ini adalah adanya trade-off antara tingkat keamanan dan kinerja real-time. Enkripsi penuh pada semua pesan GOOSE dan SMV akan memenuhi persyaratan kerahasiaan dan integritas tertinggi, tetapi akan melanggar batas latensi 4 milidetik yang dipersyaratkan. Oleh karena itu, kerangka yang diusulkan menerapkan pendekatan selektif: pesan kritis untuk proteksi (GOOSE tipe 1A) mendapatkan prioritas tertinggi dengan enkripsi ringan, sementara pesan pengukuran rutin (SMV) dilindungi melalui enkripsi sesi. Pendekatan hybrid ini terbukti berhasil menjaga latensi tetap di bawah batas standar tanpa mengorbankan keamanan secara signifikan.

4.2.4 Keterbatasan dan Tantangan Implementasi

Meskipun hasil pengujian menunjukkan kinerja yang baik, terdapat beberapa keterbatasan yang perlu diakui. Pertama, pengujian dilakukan pada lingkungan simulasi yang tidak sepenuhnya mereplikasi kondisi lapangan yang sesungguhnya, terutama dari sisi noise jaringan dan variasi beban yang tidak terduga. Kedua, model machine learning yang digunakan memerlukan data latih dari lalu lintas normal yang cukup panjang (minimal satu siklus operasi 24 jam) untuk mencapai kinerja optimal. Pada gardu yang baru beroperasi, data tersebut belum tersedia. Ketiga, skenario serangan yang diuji belum mencakup serangan zero-day yang sama sekali tidak memiliki pola yang dikenal. Untuk mengatasi hal ini, pendekatan anomaly-based

detection (tanpa memerlukan signature) sudah menjadi langkah yang tepat, namun tetap ada kemungkinan false positive yang lebih tinggi pada awal pengoperasian.

4.2.5 Implikasi bagi Operator Sistem Distribusi

Hasil penelitian ini memberikan implikasi praktis bagi operator sistem distribusi (Distribution System Operator/DSO) yang merencanakan transformasi ke gardu digital. Pertama, kerangka keamanan yang diusulkan dapat diadopsi secara bertahap, dimulai dari implementasi autentikasi mutual pada IED kritis sebelum diterapkan ke seluruh gardu. Kedua, biaya komputasi tambahan yang relatif rendah (overhead CPU 7 persen dan memori 36 MB) menunjukkan bahwa sebagian besar IED dan gateway yang ada saat ini masih mampu menjalankan kerangka ini tanpa perlu peningkatan perangkat keras. Ketiga, untuk DER yang tersebar, pendekatan federated learning memungkinkan deteksi anomali tanpa harus mengirimkan data mentah ke pusat, sehingga mengurangi risiko privasi dan bandwidth.

5. KESIMPULAN DAN SARAN

5.1 Kesimpulan

a. Kerangka keamanan yang dikembangkan berhasil mengintegrasikan tiga pilar utama, yaitu zero trust architecture (autentikasi mutual dan micro-segmentation), enkripsi ringan (AES-128-GCM dan DTLS), serta deteksi anomali berbasis ensemble machine learning (Isolation Forest dan LSTM Autoencoder). Integrasi ini terbukti mampu melindungi gardu digital dan DER dari berbagai ancaman siber modern.
b. Kinerja deteksi serangan menunjukkan hasil yang memuaskan dengan rata-rata true positive rate (TPR) mencapai 96,2 persen dan rata-rata false positive rate (FPR) hanya 2,6 persen. Serangan man-in-the-middle (MitM) memiliki tingkat deteksi tertinggi yaitu 98,1 persen, sementara serangan kombinasi (DoS dan FDI) menjadi tantangan terbesar dengan TPR 93,2 persen. Detection latency rata-rata tercatat 142,6 milidetik dan mitigation time rata-rata 0,81 detik, yang secara umum memenuhi target penelitian.
c. Overhead sistem yang ditimbulkan masih berada dalam batas toleransi untuk operasi real-time pada lingkungan OT. Tambahan penggunaan CPU sebesar 7 poin persentase, tambahan penggunaan memori sebesar 36 MB, dan tambahan latensi pesan GOOSE sebesar 1,6 milidetik (dari 1,2 ms menjadi 2,8 ms) masih memenuhi standar IEC 61850 yang mensyaratkan latensi maksimum 4 milidetik untuk pesan proteksi.
d. Pendekatan zero trust yang diimplementasikan melalui autentikasi mutual berbasis sertifikat digital X.509 dan micro-segmentation berbasis VLAN terbukti efektif

mencegah serangan MitM dan membatasi pergerakan lateral penyerang ketika satu perangkat berhasil dikompromikan. Hal ini merupakan peningkatan signifikan dibandingkan model keamanan tradisional yang hanya mengandalkan perimeter defense.

e. Pendekatan ensemble machine learning (Isolation Forest untuk deteksi cepat dan LSTM Autoencoder untuk deteksi pola temporal) terbukti lebih unggul dibandingkan penggunaan masing-masing algoritma secara terpisah. Isolation Forest efektif untuk serangan DoS dan FDI dengan perubahan drastis, sementara LSTM Autoencoder lebih baik dalam menangkap replay attack dan FDI dengan perubahan gradual (slow drift).

5.2 Saran

5.2.1 Saran untuk Penelitian Selanjutnya

a. Pengujian pada lingkungan fisik (*hardware-in-the-loop*): Penelitian selanjutnya disarankan untuk menguji kerangka keamanan pada testbed fisik dengan IED nyata dan relay proteksi sesungguhnya, bukan hanya simulasi perangkat lunak. Hal ini penting untuk memvalidasi latensi dan overhead dalam kondisi yang lebih mendekati realitas lapangan.

b. Pengembangan mekanisme deteksi untuk serangan zero-day yang lebih canggih: Meskipun pendekatan anomaly-based detection sudah baik, penelitian lebih lanjut diperlukan untuk mengembangkan mekanisme yang dapat mendeteksi serangan adversarial yang sengaja dirancang untuk mengelabui model machine learning (adversarial attacks on ML).

c. Optimasi model machine learning untuk perangkat edge dengan sumber daya sangat terbatas: Untuk DER dengan perangkat yang sangat terbatas (misalnya smart meter dengan RAM < 64 MB), diperlukan model yang lebih ringan seperti binarized neural networks atau tinyML agar kerangka keamanan tetap dapat berjalan.

d. Pengujian pada berbagai topologi jaringan dan skenario kegagalan: Penelitian selanjutnya sebaiknya menguji kerangka pada berbagai konfigurasi gardu (transmisi vs distribusi) dan skenario kegagalan komunikasi (seperti putusnya serat optik atau kegagalan switch).

5.2.2 Saran untuk Implementasi di Lapangan (Bagi Operator Sistem Distribusi / DSO)

a. Implementasi bertahap: Operator sistem distribusi disarankan untuk mengimplementasikan kerangka keamanan secara bertahap, dimulai dari gardu dengan prioritas tertinggi (misalnya yang melayani beban kritis seperti rumah sakit atau fasilitas pemerintahan). Implementasi dapat dimulai dari autentikasi mutual pada IED kritis,

kemudian dilanjutkan dengan deteksi anomali, dan terakhir enkripsi penuh pada jalur komunikasi tertentu.

b. Penyesuaian parameter deteksi anomali: Setiap gardu memiliki karakteristik lalu lintas jaringan yang berbeda. Oleh karena itu, parameter ambang batas deteksi anomali (threshold) harus disesuaikan melalui periode pembelajaran (training period) minimal 7 hari operasi normal sebelum kerangka diaktifkan sepenuhnya.
c. Penyediaan cadangan bandwidth dan daya komputasi: Meskipun overhead tergolong rendah, operator disarankan untuk menyediakan cadangan bandwidth sekitar 20 persen dan cadangan daya komputasi pada gateway gardu untuk mengakomodasi lonjakan lalu lintas atau serangan DoS yang lebih masif.
d. Pelatihan personel: Keberhasilan implementasi kerangka keamanan sangat bergantung pada kompetensi personel. Operator harus memberikan pelatihan kepada teknisi gardu dan tim siber tentang prinsip zero trust, interpretasi alarm deteksi anomali, serta prosedur respons insiden yang tepat.
e. Kolaborasi dengan vendor IED: Operator sebaiknya berkolaborasi dengan vendor IED untuk memastikan bahwa perangkat yang digunakan mendukung fitur-fitur keamanan yang diperlukan, seperti percepatan hardware untuk enkripsi AES, dukungan sertifikat digital, serta antarmuka untuk integrasi dengan sistem deteksi anomali.

DAFTAR REFERENSI

IEEE, IEEE Standard for Interconnection and Interoperability of Distributed Energy Resources with Associated Electric Power Systems Interfaces, IEEE Std 1547-2018, 2018.

IEEE, IEEE Draft Guide for Cybersecurity of Distributed Energy Resources Interconnected with Electric Power Systems, IEEE P1547.3/D7, 2021.

IEC, *Communication Networks and Systems for Power Utility Automation - Part 5: Communication Requirements for Functions and Device Models*, IEC 61850-5, Ed. 2.0, 2013.

IEC, *Power Systems Management and Associated Information Exchange - Data and Communications Security - Part 3: Communication Network and System Security - Profiles Including TCP/IP*, IEC 62351-3, Ed. 2.0, 2018.

IEC, *Power Systems Management and Associated Information Exchange - Data and Communications Security - Part 6: Security for IEC 61850*, IEC 62351-6, Ed. 1.0, 2007.

IEC, *Security for Industrial Automation and Control Systems - Part 3-3: System Security Requirements and Security Levels*, IEC 62443-3-3, Ed. 1.0, 2013.

NIST, Guide to Industrial Control Systems (ICS) Security, National Institute of Standards and Technology, NIST SP 800-82 Rev. 2, 2015.

NIST, Guidelines for Smart Grid Cybersecurity, National Institute of Standards and Technology, NIST IR 8228, 2014.

J. J. Claveria, "Integrated Testing Facilities for Digital Substation and Cyber Security based on IEC 61850 and IEC 62351 Standards," PhD thesis, Victoria University, 2025. [Online]. Available: https://vuir.vu.edu.au/49956/

J. Johnson, "P1547.3 Draft Guide for Cybersecurity Distributed Energy Resources Interconnected with Electric Power Systems," Sandia National Laboratories, Subgroup 1 Update, Feb. 2021. [Online]. Available: https://www.osti.gov/servlets/purl/1847606

O. Sen, M. A. Gurabi, M. Deruelle, A. Ulbig, and S. Decker, "Encryption-Aware Anomaly Detection in Power Grid Communication Networks," arXiv preprint arXiv:2412.04901, 2024.

A. Herath, et al., "Evaluation of Real-Time Mitigation Techniques for Cyber Security in IEC 61850 / IEC 62351 Substations," arXiv preprint arXiv:2511.18748, 2025.

RF-RADS: A Robust Framework for Risk Assessment in Digital Substations," in Proc. 2025 IEEE Conference on Communications and Network Security (CNS), Fredericton, NB, Canada, Aug. 2025.

"SDN-Based Smart Cyber Switching (SCS) for Cyber Restoration of a Digital Substation," in Proc. 2025 IEEE Power & Energy Society General Meeting (PESGM), Austin, TX, USA, Jul. 2025.

N. Hinov and S. S. Salim, "Review of Security Methods for Computer Networks in Renewable Energy Production Systems," in Proc. 2025 International Conference on Electrical Engineering and Informatics (ICEEI), Bulgaria, 2025.

C. Zenger, "From air gaps to zero-trust: Building cyber-physical resilience in the modern grid," Energy Transition Talks, CGI, Dec. 2025. [Online]. Available: https://www.cgi.com/au/en-au/podcast/energy-utilities/air-gaps-zero-trust-building-cyber-physical-resilience-modern-grid

"Real-Time Anomaly Detection: Cyber Attack Detection via SCADA Data," Renewasoft, Feb. 2026. [Online]. Available: https://renewasoft.com.tr/index.php/en/2026/02/26/real-time-anomaly-detection-cyber-attack-detection-via-scada-data/