Journal of Applied Informatics and Computing (JAIC)
Vol.x, No.x, Juli 201x, pp. xx~xx
e-ISSN: 2548-6861

Evaluasi Tingkat Kematangan Keamanan Line Produksi Operational Technology Menggunakan Pendekatan IEC 62443

Cristine Wulan Putri Siagian [1]*, Hamdani Arif [2]**
Rekayasa Keamanan Siber ,Teknik Informatika Politeknik Negeri Batam
Jl. Ahmad Yani, Tlk. Tering, kec. Batam Kota, Kota Batam, Kepulauan Riau 29461
cristine.4332201032@students.polibatam.ac.id [1] ,hamdaniarif@polibatam.ac.id [2]

Article Info

Article history:

Received …
Revised …
Accepted …

Keyword:

IEC 62443, Operational Technology, security level, security maturity,system security requirements.

ABSTRACT

The convergence of Information Technology (IT) and Operational Technology (OT) in modern manufacturing has widened the cyber attack surface of industrial control systems, making security maturity assessment essential. This study evaluates the security maturity of an OT production line (the Slice-IO line) at PT Schneider Electric Manufacturing Batam using the IEC 62443-3-3 standard. A standard-based security assessment was performed by mapping system controls to the seven Foundational Requirements (FR1-FR7), collecting evidence through documentation review, direct observation, and engineer interviews, scoring each Security Requirement on a 0-3 maturity scale, and comparing the Achieved Security Level (SL-A) against the engineer-claimed Target Security Level SL2 (SL-T). The assessment of 48 requirements shows a strong overall implementation, with an average maturity of 2.84 of 3 (94.7%). Restricted Data Flow (FR5) and Timely Response to Events (FR6) reached full implementation, while Data Confidentiality (FR4) was the weakest area at 80%. Six applicable gaps were identified, all of medium or low priority and dominated by documentation and verification needs rather than missing controls. The results indicate that the production line substantially satisfies the SL2 target, confirming the initial claim, and the study provides prioritized recommendations to consolidate SL2 and progress toward higher security levels.

I. PENDAHULUAN

Konvergensi antara Information Technology (IT) dan Operational Technology (OT) mendorong line produksi yang dahulu berdiri sendiri untuk terhubung ke jaringan perusahaan melalui lapisan OT - kumpulan Programmable Logic Controller (PLC), Human Machine Interface (HMI), sensor, dan perangkat otomasi yang mengendalikan proses fisik secara langsung [1][2]. Konektivitas ini membuka efisiensi baru, tetapi juga membuka jalur bagi ancaman siber untuk menyentuh proses produksi itu sendiri, bukan sekadar data administratif.

Konsekuensi serangan pada lingkungan OT berbeda secara kualitatif dari serangan pada sistem IT biasa. Ketika PLC dimanipulasi atau HMI kehilangan integritas datanya, dampaknya dapat berupa penghentian lini produksi, kerusakan material, hingga risiko keselamatan kerja, bukan sekadar kebocoran data [5][6]. Karakteristik inilah yang membuat pendekatan keamanan IT konvensional tidak dapat ditempelkan begitu saja ke lingkungan OT tanpa penyesuaian.

IEC 62443 hadir untuk mengisi kekosongan tersebut. Standar ini menstrukturkan keamanan sistem otomasi industri melalui pendekatan defense-in-depth: sistem dipecah menjadi zona dan conduit, lalu setiap zona diberi target ketahanan yang disebut Security Level (SL) [3]. Standar ini mendefinisikan persyaratan keamanan sistem melalui tujuh Foundational Requirement (FR1-FR7), dan setiap FR diuraikan lebih lanjut menjadi sejumlah Security Requirement (SR) yang lebih spesifik dan dapat diperiksa satu per satu terhadap bukti implementasi di lapangan [4].

Security Level bukan skor keamanan mutlak, melainkan penanda kelas ancaman yang sanggup dihadapi sistem: SL1 melindungi dari pelanggaran tidak disengaja, SL2 dari pelanggaran disengaja dengan sumber daya dan keterampilan rendah, SL3 dari serangan dengan sumber daya menengah, dan SL4 dari serangan dengan sumber daya luas dan motif tinggi [9]. SL dipakai dalam dua peran: sebagai target yang ditetapkan di awal (SL-T) dan sebagai hasil pengukuran aktual setelah evaluasi (SL-A). Penelitian ini secara khusus memperlakukan SL-T sebagai hipotesis yang harus diuji, bukan sebagai fakta yang diterima begitu saja.

Line produksi Slice-IO di PT Schneider Electric Manufacturing Batam telah memiliki klaim internal bahwa sistem OT-nya berada pada SL2, berdasarkan mekanisme CyberSecurity Manufacturing Checklist dan konfirmasi lisan dari engineer line. Namun klaim semacam ini, sepanjang belum diuji terhadap persyaratan teknis yang eksplisit, tetap berstatus asumsi. Beberapa penelitian terdahulu telah mengkaji penerapan IEC 62443, umumnya berfokus pada kerangka konseptual, pemetaan arsitektur, atau model kematangan generik, sebagaimana dirangkum pada Tabel 1.

Masih terbatas kajian yang menempuh proses verifikasi eksplisit terhadap klaim Security Level pada satu objek produksi nyata [7][8].

Berdasarkan kesenjangan tersebut, penelitian ini mengevaluasi tingkat kematangan keamanan sistem OT pada line produksi Slice-IO menggunakan pendekatan IEC 62443-3-3, dengan tujuan menentukan indikasi Achieved Security Level (SL-A) dan secara eksplisit memverifikasi apakah SL-A memenuhi atau melampaui SL-T (SL-A ≥ SL-T). Penelitian ini dirumuskan untuk menjawab dua pertanyaan: seberapa matang implementasi kontrol keamanan pada line produksi OT ditinjau dari IEC 62443, dan gap keamanan apa saja yang masih membutuhkan perbaikan.

Tujuan penelitian mengikuti kedua pertanyaan tersebut, yaitu mengukur tingkat kematangan implementasi kontrol keamanan, memverifikasi kesesuaian SL-A terhadap SL-T, dan menyusun rekomendasi perbaikan berbasis gap analysis. Adapun kontribusi penelitian ini adalah tersedianya verifikasi terukur atas klaim SL2 pada line Slice-IO beserta jejak bukti (audit trail) yang dapat ditelusuri ulang, alih-alih sekadar deskripsi implementasi keamanan yang bersifat naratif.

Tabel 1. Perbandingan Penelitian Sebelumnya

Research Gap

Peneliti (Tahun)	Fokus & Metode	Hasil Utama	Keterbatasan Metodologis
Cindric et al. (2025)	Systematic mapping IEC 62443 pada IIoT	IEC 62443 efektif untuk evaluasi & identifikasi gap	Systematic mapping bersifat konseptual, tanpa verifikasi pada objek produksi nyata
Goettel et al. (2023)	Qualitative analysis kebutuhan keamanan ICS	Konvergensi IT/OT meningkatkan kebutuhan evaluasi standar	Analisis kualitatif, tidak menghasilkan skor kuantitatif yang dapat direplikasi
Brancati et al. (2025)	Risk-based assessment ICS berbasis IEC 62443	ICS perlu evaluasi berkelanjutan sesuai kematangan	Fokus pada penilaian risiko, tanpa kriteria keputusan biner SL-A vs SL-T eksplisit
Cosman et al. (2023)	Security maturity model berbasis IEC 62443	Pemetaan maturity membantu identifikasi gap	Model kematangan generik, belum diuji pada satu objek line produksi spesifik
Karnouskos (2021)	Framework analysis implementasi IEC 62443	Terdapat gap implementasi aktual vs. keamanan yang diharapkan	Analisis framework literatur, tanpa pengumpulan bukti primer dari sistem nyata
Penelitian ini (2026)	Standard-based assessment + verifikasi SL-A vs SL-T	SL-A ≥ SL-T terverifikasi; 8 gap minor teridentifikasi	Cakupan satu line produksi, tanpa pengujian teknis langsung

Berdasarkan penelitian sebelumnya, sebagian besar penelitian hanya berfokus pada identifikasi risiko atau pengukuran tingkat keamanan tanpa melakukan pemetaan implementasi Security Requirement IEC 62443-3-3 hingga penentuan Security Level Actual (SL-A). Selain itu, penelitian terdahulu belum secara spesifik mengevaluasi line produksi pada lingkungan OT menggunakan seluruh Foundational Requirement (FR1–FR7). Oleh karena itu, penelitian ini melakukan evaluasi implementasi seluruh Security Requirement yang applicable, menghitung tingkat pencapaian Security Level Actual, serta menyusun rekomendasi peningkatan keamanan berdasarkan hasil gap analysis.

II. METODE

A. Pendekatan Penelitian

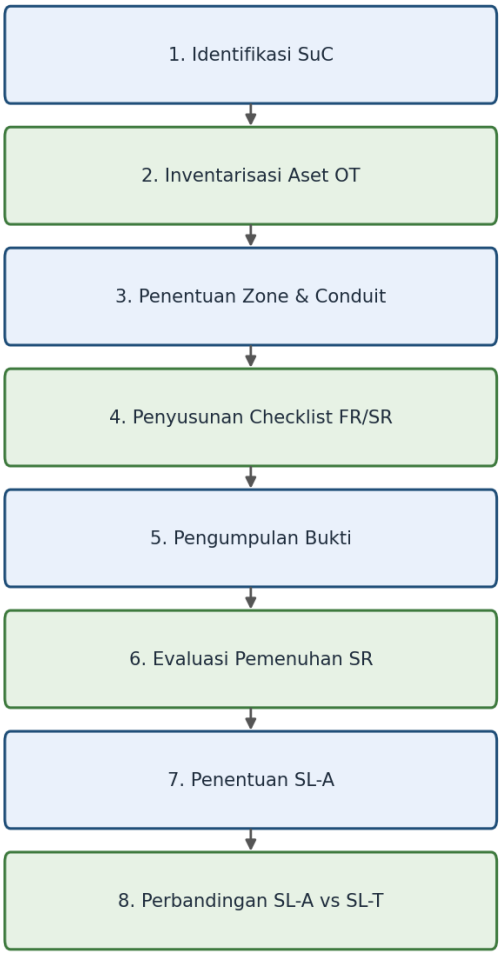
Penelitian ini menggunakan pendekatan studi kasus evaluatif-deskriptif melalui metode standard-based security assessment, dipilih karena objek penelitian merupakan sistem produksi aktif yang berisiko terganggu apabila diuji melalui pendekatan agresif seperti penetration testing. Objek evaluasi adalah sistem OT pada line produksi Slice-IO, dengan Target Security Level (SL-T) pada SL2 sebagaimana ditetapkan melalui mekanisme internal CyberSecurity Manufacturing Checklist dan dikonfirmasi melalui wawancara awal bersama engineer line produksi.

Variabel yang dievaluasi dalam penelitian ini adalah tingkat pemenuhan setiap Security Requirement (SR) pada tujuh Foundational Requirement (FR1-FR7) sesuai IEC 62443-3-3. Indikator yang diukur meliputi rata-rata skor kematangan per FR, persentase pemenuhan, jumlah dan prioritas gap yang ditemukan, serta status akhir perbandingan SL-A terhadap SL-T. Kondisi pengujian dikendalikan dengan membatasi lingkup evaluasi hanya pada satu line produksi dan satu periode observasi, agar bukti yang dikumpulkan tetap konsisten dan dapat ditelusuri.

B. Tahapan Penelitian

Proses evaluasi ditempuh melalui delapan tahapan berurutan sebagaimana diilustrasikan pada Gambar 1.

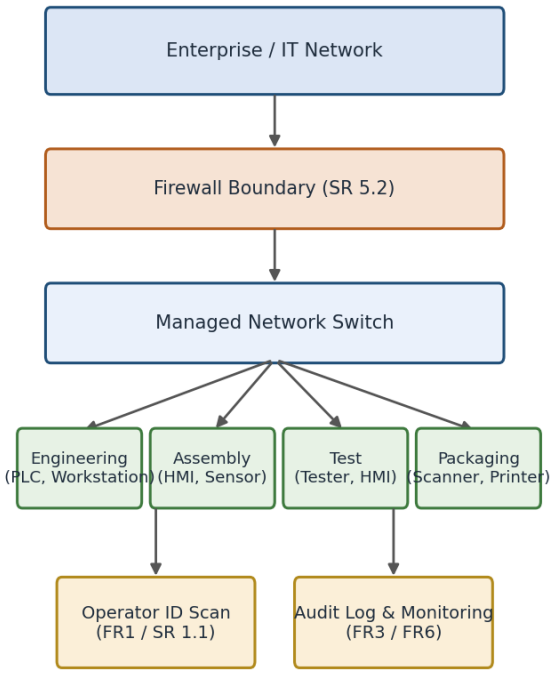
- Identifikasi System Under Consideration (SuC): menetapkan batas sistem OT line Slice-IO beserta komponen PLC, HMI, workstation engineering, dan jaringan komunikasinya.
- Inventarisasi aset OT: PLC, HMI, workstation engineering, managed switch, perangkat identifikasi (barcode/RFID), dan perangkat otomasi lain yang terintegrasi.
- Penentuan zone dan conduit mengikuti konsep segmentasi IEC 62443, memetakan aset ke dalam kelompok dengan kebutuhan keamanan serupa serta jalur komunikasi antar-zona [10].
- Penyusunan checklist evaluasi IEC 62443-3-3, memetakan kontrol terhadap FR1-FR7 dan SR pada Capability Security Level yang relevan.
- Pengumpulan bukti implementasi melalui tiga jalur yang saling melengkapi: studi dokumentasi, observasi langsung, dan wawancara dengan engineer pengelola sistem.
- Evaluasi pemenuhan setiap SR berdasarkan bukti yang terkumpul, kemudian dikelompokkan menurut kategori FR.
- Penentuan Achieved Security Level (SL-A) dengan menghitung rata-rata pemenuhan SR pada tiap FR.
- Perbandingan SL-A terhadap SL-T menggunakan kriteria keputusan eksplisit, dilanjutkan dengan gap analysis sebagai dasar rekomendasi.



Gambar 1. Diagram Alir Tahapan Penelitian

C. Objek dan Arsitektur Evaluasi

Objek evaluasi adalah line produksi Slice-IO yang digunakan dalam manufaktur modul otomasi industri. Arsitektur konseptualnya digambarkan pada Gambar 2: line ini tersusun atas empat sub-area utama, yaitu Engineering, Assembly, Test, dan Packaging, yang terhubung melalui managed network switch dan dibatasi dari jaringan enterprise oleh firewall boundary. Setiap sub-area memiliki kombinasi PLC, HMI, atau workstation yang menjadi titik pemeriksaan checklist, sementara identifikasi pengguna (Operator ID) dan mekanisme audit log berlaku lintas seluruh sub-area sebagai kontrol yang bersifat menyeluruh.



Gambar 2. Arsitektur Konseptual Sistem OT pada Line Produksi Slice-IO

Pembagian sistem menjadi zone dan conduit menjadi dasar penentuan lingkup evaluasi FR5 (Restricted Data Flow). Sebuah zone adalah kelompok aset yang berbagi kebutuhan keamanan setara, sedangkan conduit adalah jalur komunikasi yang menghubungkan antar-zone. Pada line Slice-IO, zone Enterprise/IT dan zone OT dipisahkan oleh firewall boundary yang berfungsi sebagai conduit terkontrol; pemisahan inilah yang diperiksa pada SR 5.1 dan SR 5.2.

D. Skema Penilaian

Setiap Security Requirement dinilai pada skala kematangan 0-3: 0 untuk kontrol yang tidak diterapkan, 1 untuk kontrol yang diterapkan sebagian, 2 untuk kontrol yang diterapkan dengan bukti memadai, dan 3 untuk kontrol yang diterapkan dengan bukti kuat dan konsisten lintas sumber.

Skala empat tingkat ini bukan ketentuan baku dari IEC 62443-3-3, melainkan instrumen penilaian kematangan yang diadaptasi dari pendekatan capability-based scoring yang lazim digunakan pada model pengukuran keamanan siber terapan, sejalan dengan struktur Capability Maturity Model (CMM) [12], model kematangan keamanan siber nasional Karabacak dkk. [13], kerangka penilaian kematangan kapabilitas siber Liyanage dkk. [14], serta instrumen Indeks Keamanan Informasi (Indeks KAMI) yang diterbitkan Badan Siber dan Sandi Negara [15]. Keempat rujukan tersebut secara konsisten menggunakan rentang skor bertingkat untuk membedakan derajat implementasi kontrol, bukan sekadar status diterapkan/tidak diterapkan, sehingga pendekatan serupa diadopsi pada penelitian ini agar tingkat kematangan tiap SR dapat dibandingkan secara proporsional antar-FR.

SR yang tidak relevan terhadap lingkup ditandai Not Applicable (NA) dan dikeluarkan dari perhitungan rata-rata. Rata-rata skor pada tiap FR dihitung menggunakan Persamaan (1), dan persentase pemenuhannya menggunakan Persamaan (2).

$$\bar{S}\_FR = (\Sigma s_i) / n \quad (1)$$

dengan s_i adalah skor SR ke-i yang berstatus applicable pada suatu FR, dan n adalah jumlah SR applicable pada FR tersebut.

$$P\_FR = (\bar{S}\_FR / 3) \times 100\% \quad (2)$$

Skor 2 pada penelitian ini dapat muncul dari dua kondisi yang secara konsep berbeda, yaitu (a) kontrol sudah

diimplementasikan secara teknis namun baru mencakup sebagian dari cakupan yang seharusnya, dan (b) kontrol sudah berjalan penuh secara operasional, tetapi bukti pendukungnya belum dapat diverifikasi secara teknis menyeluruh, misalnya karena pengujian langsung berada di luar kewenangan akses peneliti. Kedua kondisi ini tetap dicatat dengan angka skor yang sama untuk menjaga konsistensi perhitungan SL-A, namun dibedakan melalui catatan kualitatif pada checklist evaluasi sehingga pembaca dapat menelusuri alasan spesifik di balik tiap skor 2 yang diberikan.

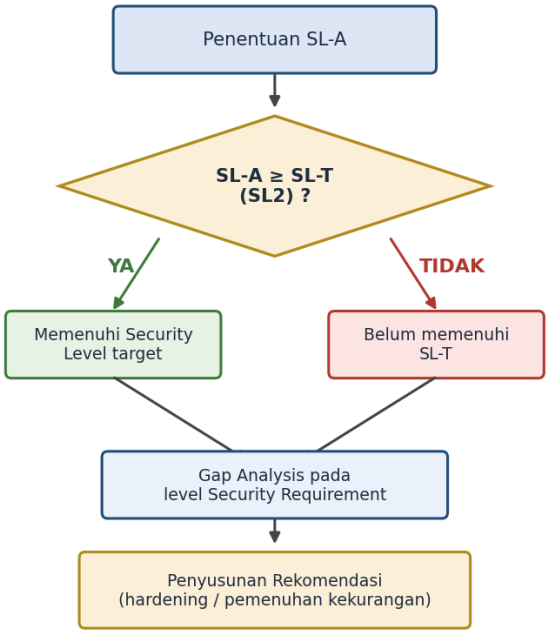
Sebagai ilustrasi: SR 1.1 (Human User Identification) memperoleh skor 3 karena bukti dokumen (SOP login), observasi (tangkapan layar permintaan Operator ID Scan pada HMI), dan konfirmasi lisan dari engineer seluruhnya konsisten menunjukkan setiap operator wajib teridentifikasi sebelum proses berjalan. Sebaliknya, SR 4.3 (Encryption of Data in Transit) memperoleh skor 2 pada kondisi (b): observasi menunjukkan konfigurasi segmentasi jaringan konsisten dengan praktik enkripsi standar, namun pengujian teknis langsung seperti traffic capture berada di luar kewenangan akses peneliti sehingga konfirmasi eksplisit bahwa data yang melintas benar-benar terenkripsi belum dapat dilakukan, sehingga item ini dicatat sebagai gap meskipun skornya di atas ambang minimum.

Kedua contoh di atas hanya mewakili pola skor tertinggi dan skor bermasalah untuk menggambarkan mekanisme penilaian. Skor lengkap beserta jejak bukti (audit trail) untuk seluruh 44 SR applicable, mencakup kode SR, skor, kategori bukti, dan catatan kualitatif, disajikan pada Lampiran A dan dapat ditelusuri ulang melalui checklist evaluasi yang menyertai penelitian ini.

E. Kriteria Penentuan SL-A dan Perbandingan dengan SL-T

Ambang minimum SL2 dirumuskan secara eksplisit sebagai berikut: suatu FR dinyatakan memenuhi SL2 apabila $\bar{S}\_FR \geq 2{,}0$ dari skala 0-3, setara dengan $P\_FR \geq 67\%$. Angka ini merujuk pada konvensi capability-based scoring sebagaimana diuraikan pada Bagian II.D [12][13][14][15], di mana skor 2 merepresentasikan kontrol yang sudah diterapkan dengan bukti memadai, dipandang sebagai batas bawah yang cukup untuk pertahanan terhadap ancaman dengan sumber daya dan keterampilan rendah sesuai definisi SL2 [9].

Inti dari seluruh proses evaluasi bermuara pada satu keputusan biner yang digambarkan pada Gambar 3: apakah SL-A yang terukur lebih besar atau sama dengan SL-T (SL2)? Sistem dinyatakan memenuhi SL-T hanya apabila seluruh tujuh kategori FR memenuhi ambang minimum ($P\_FR \geq 67\%$) secara serentak, bukan rata-rata gabungan semua FR, karena satu FR yang lemah semestinya tidak bisa "ditutupi" oleh FR lain yang kuat.



Gambar 3. Diagram Logika Perbandingan SL-A dengan SL-T

Kedua cabang keputusan pada Gambar 3, baik "Ya" maupun "Tidak", tetap bermuara pada gap analysis dan penyusunan rekomendasi. Perbedaannya terletak pada sifat rekomendasi: jika $SL\text{-}A \geq SL\text{-}T$, gap yang ditemukan bersifat penguatan (hardening) menuju level berikutnya; jika $SL\text{-}A < SL\text{-}T$, gap tersebut adalah kekurangan mendasar yang harus dipenuhi lebih dulu agar SL-T tercapai.

F. Instrumen dan Triangulasi Bukti

Setiap Security Requirement diusahakan memperoleh bukti dari lebih dari satu jalur pengumpulan data agar penilaian tidak bersandar pada satu sudut pandang saja. Studi dokumentasi mencakup SOP, Work Instruction, dan diagram arsitektur jaringan; observasi langsung mencakup pemeriksaan konfigurasi PC/PLC, tangkapan layar Event Viewer, dan status endpoint protection; sedangkan wawancara dilakukan bersama engineer line produksi untuk mengonfirmasi praktik yang tidak selalu tampak dari dokumen atau layar semata. Ringkasan sebaran jenis bukti disajikan pada Tabel 2.

Tabel 2. Ringkasan Sumber Bukti

Sumber	Cakupan FR	Kegunaan Utama
Dokumen	FR1,2,4,5,7	Verifikasi keberadaan prosedur formal
Observasi	FR1,2,3,6,7	Verifikasi implementasi aktual di lapangan
Wawancara	FR1,3,4,6,7	Melengkapi konteks di luar dokumen/observasi

G. Analisis Data

Analisis dilakukan secara komparatif antara nilai kematangan per FR terhadap ambang minimum SL2, dilengkapi statistik deskriptif sederhana (rata-rata dan persentase) untuk menggambarkan kecenderungan hasil.

H. Mitigasi Bias Penilai dan Verifikasi Independen

Klaim SL-T awal serta sebagian besar informasi kontekstual pada penelitian ini diperoleh dari CyberSecurity Manufacturing Checklist internal dan wawancara dengan engineer line produksi. Agar skor akhir tidak semata bersandar pada pernyataan pihak yang mengelola line tersebut, peneliti tidak menerima keterangan supervisor/lead secara langsung sebagai skor final, melainkan menempuh dua langkah verifikasi tambahan. Pertama, setiap klaim lisan dicocokkan dengan bukti independen berupa dokumen SOP, tangkapan layar konfigurasi, dan observasi langsung di lapangan, serta dibandingkan terhadap persyaratan teknis pada IEC 62443-3-3 yang dipelajari dan diinterpretasikan sendiri oleh peneliti, bukan mengikuti penafsiran engineer line. Kedua, skoring awal dan penetapan prioritas gap dikaji ulang oleh Pak Yudha Baskara Setiawan (Test and Maintenance Manager) Kaji ulang dilakukan dengan memeriksa kembali bukti untuk setiap SR sebelum skor difinalisasi apabila terdapat perbedaan penilaian, skor final ditetapkan melalui diskusi konsensus dengan bukti sebagai rujukan utama. Mekanisme ini ditujukan untuk mengurangi risiko bias konfirmasi yang dapat timbul dari kedekatan peneliti dengan tim operasional selama pengumpulan data.

III. HASIL DAN PEMBAHASAN

3.1 Profil Sistem dan Ringkasan Evaluasi

Line produksi Slice-IO memasuki evaluasi dengan status SL-T = SL2, hasil penetapan internal perusahaan yang menjadi acuan pembanding sepanjang penelitian. Evaluasi mencakup 48 Security Requirement yang tersebar pada tujuh

Tabel 3. Rekapitulasi Tingkat Kematangan per FR

FR	Skor	%	Gap
FR1	2,83	94,3	1
FR2	2,60	86,7	2
FR3	2,89	96,3	1
FR4	2,40	80,0	2
FR5	3,00	100	0
FR6	3,00	100	0
FR7	3,00	100	0
Total	**2,84**	**94,7**	**6**

Keterangan: FR1 Identification & Authentication Control; FR2 Use Control; FR3 System Integrity; FR4 Data Confidentiality; FR5 Restricted Data Flow; FR6 Timely Respo nse to Events; FR7 Resource Availability.

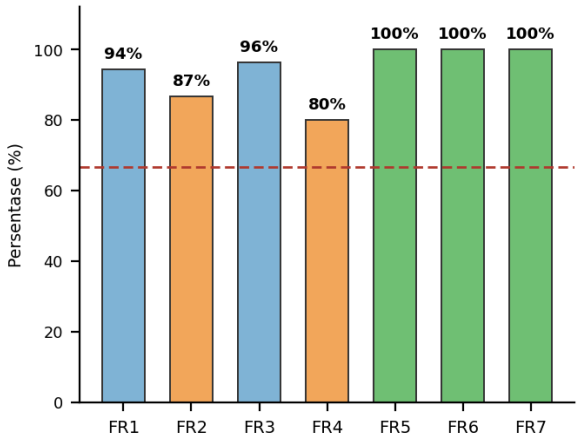
Untuk data gap, analisis dilakukan secara kualitatif dengan mengelompokkan temuan berdasarkan prioritas (tinggi/sedang/rendah) yang ditetapkan bersama engineer line produksi, sehingga rekomendasi dapat diurutkan sesuai urgensi perbaikan.

FR sebagaimana diuraikan pada Bab II. Dari jumlah tersebut, 44 item dinilai applicable dan 4 item berstatus Not Applicable, yaitu autentikasi nirkabel (SR 1.6), Public Key Infrastructure (SR 1.8), kendali penggunaan nirkabel (SR 2.2), dan kendali sesi bersamaan (SR 2.7).

Agar status kesesuaian setiap SR tidak hanya dibaca sebagai dua kategori kasar (Applicable/Not Applicable), keempat SR berstatus NA di atas dibedakan menurut alasan penetapannya, bukan sekadar dicatat sebagai NA generik. SR 1.6 dan SR 2.2 ditetapkan NA-Arsitektural karena SuC memang tidak mengimplementasikan komunikasi nirkabel dalam bentuk apa pun — seluruh jalur PLC-HMI-Workstation bersifat wired melalui managed switch (Gambar 2) — sehingga kontrol autentikasi maupun kendali penggunaan nirkabel tidak relevan diterapkan, bukan luput dari pengujian. SR 1.8 ditetapkan NA-Arsitektural karena skema autentikasi pada line ini menggunakan Operator ID berbasis akun, bukan sertifikat digital/PKI, sesuai kompleksitas kontrol yang dipersyaratkan pada SL2. SR 2.7 ditetapkan NA-Fungsional karena platform SCADA/HMI yang digunakan tidak menyediakan fitur teknis untuk membatasi sesi berganda, sehingga secara formal berada di luar kapabilitas sistem untuk dikendalikan. Butir SR 2.7 tetap dicatat sebagai catatan gap karena ditemukan indikasi risiko terkait, meskipun secara formal berstatus NA pada lingkup evaluasi ini.

3.2 Rekapitulasi Tingkat Kematangan per Foundational Requirement

Hasil rekapitulasi tingkat kematangan tiap FR, dihitung menggunakan Persamaan (1) dan (2), disajikan pada Tabel 3 dan divisualisasikan pada Gambar 4.



Gambar 4. Grafik Tingkat Kematangan Keamanan per FR

Pola yang segera terlihat pada Gambar 4 adalah tidak satu pun FR yang jatuh di bawah ambang minimum SL2 (P_FR = 67%, sebagaimana dirumuskan pada Bagian II.E), bahkan domain terlemah sekalipun (FR4, 80%) masih jauh di atas

garis tersebut. Enam gap yang ditemukan tersebar di empat dari tujuh FR, seluruhnya berprioritas sedang atau rendah tanpa satu pun berprioritas tinggi.

3.2.1 Domain dengan Capaian Tertinggi

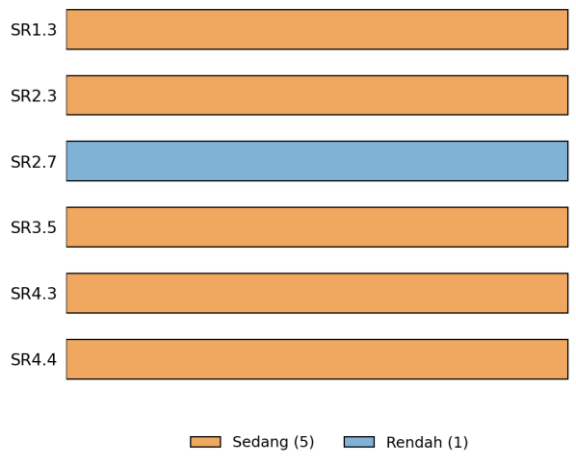
Pembatasan aliran data (FR5) dan respons tepat waktu terhadap kejadian (FR6) mencapai implementasi penuh (100%). Pada FR5, segmentasi jaringan, proteksi batas zona, dan prinsip deny-by-default berjalan konsisten, sejalan dengan arsitektur zona pada Gambar 2. Pada FR6, aksesibilitas audit log, monitoring berkelanjutan, dan mekanisme alarm seluruhnya terpenuhi, didukung observasi langsung terhadap Windows Event Viewer yang mencatat log aktivitas lengkap dengan identitas akun pengguna.

3.2.2 Domain dengan Formalisasi Tertinggal

Identifikasi dan autentikasi (FR1, 94,3%), kendali penggunaan (FR2, 86,7%), dan integritas sistem (FR3, 96,3%) menunjukkan pola serupa: kontrol inti sudah berjalan, namun formalisasi dokumentasinya tertinggal. Pada FR1, operator diwajibkan melakukan scan Operator ID sebelum proses produksi berjalan, dan mekanisme autentikasi perangkat pada workstation engineering sudah cukup terbatas pada personel tertentu; satu-satunya celah yang tersisa adalah dokumentasi review akun berkala (SR 1.3) yang belum tersedia secara formal. Pada FR2, penggunaan perangkat portabel belum diatur prosedur baku (SR 2.3), dan ditemukan penggunaan satu akun yang sama pada beberapa PC line (SR 2.7) sehingga sesi individual sulit ditelusuri. Pada FR3, validasi input (SR 3.5) berjalan namun dokumentasinya belum lengkap.

Tabel 4. Ringkasan Gap dan Rekomendasi

SR	Temuan & Rekomendasi	Prio.
1.3	Review akun belum terdokumentasi → susun prosedur berkala.	Sedang
2.3	Perangkat portabel belum diatur → susun SOP pemeriksaan.	Sedang
2.7	Akun dipakai bersama → migrasi ke akun individual.	Rendah
3.5	Validasi input belum terdokumentasi → lengkapi dokumentasi.	Sedang
4.3	Enkripsi transit belum terverifikasi → pastikan protokol terenkripsi.	Sedang
4.4	Enkripsi data tersimpan belum terverifikasi → verifikasi & dokumentasikan.	Sedang



Gambar 5. Distribusi Prioritas Enam Gap Hasil Evaluasi

Lima dari enam gap berprioritas sedang dan satu berprioritas rendah, tanpa satu pun berprioritas tinggi. Pola ini menunjukkan bahwa seluruh gap yang ditemukan berakar pada kekurangan dokumentasi dan formalisasi prosedur, bukan pada ketiadaan kontrol keamanan itu sendiri.

3.2.3 Domain dengan Capaian Terendah

Kerahasiaan data (FR4) menjadi domain dengan capaian terendah (80%). Perlindungan dasar tersedia melalui pembatasan akses berbasis akun, namun dua persyaratan intinya, yaitu enkripsi data saat transit (SR 4.3) dan data tersimpan/data-at-rest (SR 4.4), termasuk kondisi (b) sebagaimana didefinisikan pada Bagian II.D: konfigurasi dan segmentasi jaringan yang teramati konsisten dengan praktik enkripsi standar, namun pengujian teknis independen atas kedua SR tersebut belum dapat dilakukan sepenuhnya karena berada di luar kewenangan akses peneliti. Posisi FR4 sebagai domain terlemah ini konsisten dengan pola umum pada sistem OT, di mana kontrol akses lebih mudah diimplementasikan lebih dulu dibanding kontrol kriptografis yang membutuhkan penyesuaian arsitektur komunikasi lebih dalam [6]. Ketersediaan sumber daya (FR7, 100%) tidak menyisakan gap sama sekali, termasuk pada proteksi Denial of Service (SR 7.1) yang mekanisme pembatasan aksesnya sudah berjalan dan terverifikasi memadai.

3.3 Analisis Gap dan Prioritas Perbaikan

Ringkasan seluruh enam gap beserta rekomendasi perbaikannya disajikan pada Tabel 4, dan distribusi prioritasnya divisualisasikan pada Gambar 5.

3.4 Penentuan SL-A dan Verifikasi terhadap SL-T

Merujuk kriteria keputusan pada Gambar 3, penentuan SL-A dilakukan dengan memeriksa apakah seluruh kategori FR mencapai ambang minimum SL2 secara serentak. Tabel 3 menunjukkan ketujuh FR memiliki rata-rata skor antara 2,40 dan 3,00 dari skala 0-3 (80% hingga 100%), dan tidak satu pun gap berprioritas tinggi ditemukan. Karena syarat tersebut terpenuhi tanpa pengecualian, indikasi Achieved Security Level (SL-A) sistem berada pada SL2.

Dengan demikian, jawaban atas pertanyaan penelitian - apakah SL-A ≥ SL-T? - adalah YA. SL-A (SL2) sekurang-kurangnya setara dengan SL-T (SL2) yang diklaim sebelumnya, sehingga klaim awal engineer line produksi terverifikasi oleh evaluasi berbasis IEC 62443-3-3. Mengikuti cabang "Ya" pada Gambar 3, sistem dinyatakan memenuhi Security Level yang ditargetkan, meskipun enam gap pada Tabel 4 tetap direkomendasikan perbaikannya sebagai langkah penguatan (hardening) menuju Security Level berikutnya, bukan sebagai kekurangan yang menggagalkan pemenuhan SL2 saat ini.

3.5 Keterkaitan Temuan dengan Penelitian Terdahulu

Dibandingkan dengan pola pada Tabel 1, temuan ini memperkuat sekaligus melengkapi observasi Karnouskos [8] bahwa umumnya masih terdapat gap antara implementasi aktual dan tingkat keamanan yang diharapkan pada sistem industri. Perbedaannya, penelitian ini menunjukkan bahwa

keberadaan gap tidak selalu berarti target keamanan gagal terpenuhi, selama gap tersebut berada di bawah ambang yang memengaruhi status kelulusan tiap FR. Hal ini sejalan dengan pendekatan model kematangan Cosman et al. [7], yang menekankan bahwa pemetaan maturity terhadap IEC 62443 berguna untuk mengidentifikasi gap secara presisi, bukan untuk menyimpulkan lulus-tidaknya secara biner tanpa nuansa.

IV. KESIMPULAN

Penelitian ini memverifikasi klaim Security Level pada line produksi Slice-IO di PT Schneider Electric Manufacturing Batam melalui evaluasi standard-based berbasis IEC 62443-3-3. Dari 48 Security Requirement yang dievaluasi, 44 di antaranya applicable dengan rata-rata kematangan 2,84 dari 3 (94,7%). Seluruh tujuh kategori Foundational Requirement mencapai ambang minimum SL2 tanpa satu pun gap berprioritas tinggi, sehingga jawaban atas pertanyaan penelitian adalah SL-A $\geq$ SL-T terpenuhi, memverifikasi klaim awal engineer line produksi secara empiris.

Enam gap yang ditemukan seluruhnya berakar pada kekurangan dokumentasi, formalisasi prosedur, dan verifikasi teknis enkripsi data, bukan ketiadaan kontrol keamanan mendasar. Rekomendasi yang disusun diarahkan untuk mengonsolidasikan pemenuhan SL2 sekaligus menjadi fondasi menuju Security Level yang lebih tinggi, dengan prioritas pada penguatan kerahasiaan data (FR4) dan akuntabilitas akun pengguna (SR 2.7).

Penelitian ini memiliki keterbatasan pada cakupan satu line produksi dan bukti yang bersifat non-intrusif (dokumentasi, observasi, wawancara) tanpa pengujian teknis langsung seperti vulnerability scanning, karena kewenangan tersebut berada pada tim keamanan siber internal perusahaan. Penelitian lanjutan disarankan memperluas cakupan ke beberapa line produksi sekaligus, serta memadukan hasil assessment ini dengan pengujian teknis terkendali untuk memverifikasi temuan gap secara lebih mendalam, khususnya pada domain kerahasiaan data yang menjadi capaian terendah pada penelitian ini.

UCAPAN TERIMA KASIH

Penulis mengucapkan terima kasih kepada Politeknik Negeri Batam dan PT Schneider Electric Manufacturing Batam atas dukungan, akses data, serta kesempatan yang diberikan selama pelaksanaan penelitian ini.

Daftar Pustaka

[1] B. Leander, A. Causevic, and H. Hansson, "Applicability of the IEC 62443 standard in Industry 4.0/IIoT," in Proc. 14th Int. Conf. on Availability, Reliability and Security (ARES '19), 2019.

[2] I. Cindric, M. Jurcevic, and T. Hadjina, "Mapping of Industrial IoT to IEC 62443 standards," Sensors, vol. 25, no. 3, art. 728, 2025.

[3] International Electrotechnical Commission, IEC 62443: Industrial Communication Networks – IT Security for Networks and Systems. Geneva, Switzerland: IEC.

[4] Cisco, "What is IEC 62443?" Cisco Cybersecurity Guide, 2024.

[5] F. Brancati, D. Mongelli, F. Mariotti, and P. Lollini, "A cybersecurity risk assessment methodology for industrial automation control systems," Int. J. Inf. Security, vol. 24, art. 76, 2025.

[6] C. Goettel et al., "Qualitative analysis for validating IEC 62443-4-2 requirements in DevSecOps," in Proc. IEEE Int. Conf. on Industrial Cyber-Physical Systems (ICPS), 2023.

[7] E. Cosman et al., IoT Security Maturity Model: ISA/IEC 62443 Mappings. International Society of Automation (ISA), 2023.

[8] A. Karnouskos, "Industrial cyber-physical system security," IEEE Industrial Electronics Magazine, vol. 15, no. 1, 2021.

[9] K. Stouffer, V. Pillitteri, S. Lightman, M. Abrams, and A. Hahn, Guide to Industrial Control Systems (ICS) Security, NIST SP 800-82 Rev. 2, 2015.

[10] T. Hardiana and S. Suhardi, "Desain Instrumen Pengukuran Tingkat Kematangan Keamanan Siber Sektor Pemerintahan," Jurnal Pendidikan dan Teknologi Indonesia, vol. 5, no. 11, pp. 3288-3305, 2025.

[11] ISA Global Cybersecurity Alliance (ISAGCA), Quick Start Guide: An Overview of ISA/IEC 62443 Standards. ISAGCA.

[12] M. C. Paulk, B. Curtis, M. B. Chrissis, and C. V. Weber, "Capability Maturity Model for Software, Version 1.1," Software Engineering Institute, Carnegie Mellon University, Pittsburgh, PA, USA, Tech. Rep. CMU/SEI-93-TR-024, 1993.

[13] B. Karabacak, S. Ozkan Yildirim, and N. Baykal, "A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness," Int. J. Critical Infrastructure Protection, vol. 15, pp. 47-59, 2016.

[14] L. Liyanage, N. Arachchilage, and G. Russello, "A Novel Framework to Assess Cybersecurity Capability Maturity," in Proc. 33rd European Conf. on Information Systems (ECIS 2025), Amman, Jordan, 2025.

[15] Badan Siber dan Sandi Negara (BSSN), Panduan Indeks Keamanan Informasi (Indeks KAMI), BSSN, Jakarta, Indonesia, 2023.