*Syntax Literate:* Jurnal Ilmiah Indonesia p–ISSN: 2541-0849
e-ISSN : 2548-1398
Vol. 4, No. 4 April 2019

# PENILAIAN RESIKO KEAMANAN INFORMASI PADA INFRASTRUKTUR KRITIS SISTEM SCADA AREA PENGATUR BEBAN XXX BERDASARKAN PANDUAN NIST SP 800-82

**Oscar Hadikaryana dan Aswin Sasongko**
Universitas Kebangsaan, Bandung; Universitas Langlangbuana, Bandung
Email: oscar@universitas.kebangsaan.ac.id; Ashwin.sasongko@gmail.com.

**Abstrak**

*Seperti diketahui, kebutuhan listrik Indonesia meningkat setiap tahun, PLN sebagai perusahaan yang mendistribusikan listrik ke pelanggan. Untuk memenuhi hal ini, PLN mengelola distribusi daya dari pembangkit listrik ke pelanggan melalui gardu induk yang tersebar di Jawa-Bali dan pulau-pulau lain, kebutuhan sistem aplikasi SCADA sebagai regulator beban terintegrasi telah digunakan oleh PLN sejak lama. Tujuan peneltian ini adalah perusahaan mengetahui dan mendapatkan peta resiko (risk) serta dampak (impact) dalam potensi kerawanan (vulnerability) di sistem SCADA khususnya XXX. Berikutnya PLN dapat menyususun rencana keamanan berdasarkan identifikasi kelemahan dan kerawanan teknologi informasi SCADA dan dapat melanjutkan ke tahap berikutnya yaitu mitigasi risiko teknologi informasi SCADA. Sehingga PLN dapat menyusun strategi dalam mengantisipasi ancaman gangguan dan serangan terhadap aset perusahaan terutama SCADA APB Cigereleng. APB (Area Kontrol Beban) adalah operator pengatur beban yang mengoperasikan Sistem SCADA yang tersebar di beberapa area distribusi. Karena ini menyangkut kebutuhan energi banyak orang, sistem SCADA diklasifikasikan sebagai infrastruktur kritis. Sehingga dalam operasi memerlukan penilaian risiko, terutama dalam hal keamanan informasi SCADA, sebagai bagian dari manajemen risiko.*

**Kata kunci** : *SCADA, Risk Assessment, NIST, Ancaman, Kerentanan*

## Pendahuluan

Risk Assessment adalah kegiatan terpenting yang dilakukan didalam Sistem Manajemen Keamanan Informasi di infrastruktur kritis seperti PLN, melalui penilaian resiko ini organisasi dapat memahami seberapa besar dampak yang akan diterima PLN jika terjadi kejadian Keamanan Informasi pada sistem kendali industri yang digunakan yaitu sistem SCADA. Menurut kajian BPPT dalam Outlook Energi Nasional 2014 [1], dimana PLN sebagai salah satu perusahaan infrastruktur kritis yang pada tahun 2015 , harus mendistribusikan listrik nasional dari pembangkit listrik ke konsumen sebesar 252

TWh antara 256 TWh. Dengan perkiraan kebutuhan listrik pada tahun 2015 adalah 222 TWh sampai 305 TWh pada tahun 2019. Dimana sektor industri diperkirakan memanfaatkan listrik sebesar 40 % - 44 % daya terpasang, sektor rumah tangga sebesar 35 % dan transportasi 0,1 % s/d 0,2 %.

Walaupun menurut NIST [2] ada perbedaan karakteristik antara sistem teknologi informasi ( IT) tradisional dan sistem kendali industri (ICS) seperti perbedaan resiko dan prioritas. Yang terpenting adalah risiko kesehatan dan keselamatan hidup manusia, kerusakan serius pada lingkungan dan kehilangan produksi yang menyebabkan kerugian keungan serta akibat negatip kepada ekonomi nasional.

Menurut Rokhimatul Wakhidah [3] : Keamanan informasi menjadi isu yang sangat penting bagi perusahaan penyedia listrik. Berdasarkan penilaian para ahli, listrik merupakan salah satu infrastruktur kritis dan merupakan fokus target penyerangan yang menempati urutan lima besar di seluruh dunia. SCADA di PLN berfungsi mulai dari pengambilan data pada peralatan pembangkit atau gardu induk, pengolahan informasi yang diterima, sampai reaksi yang ditimbulkan dari hasil pengolahan informasi.

Dengan adanya peralatan SCADA penyampaian dan pemrosesan data dari sistem tenaga listrik akan lebih cepat diketahui oleh operator (*dispatcher*). Informasi pengukuran dan status indikasi dari sistem tenaga listrik dikumpulkan dengan menggunakan peralatan yang ditempatkan di gardu induk dan di pusat pembangkit. Kontrol penyaluran sistem peralatan memungkinkan penyampaian data secara *remote*. Data yang baru dapat juga dihitung dan disimpan dalam data base melalui pengumpulan nilai secara automatis. Penyampaian data dan pemrosesan data dilakukan secara *real-time*. Parameter sistem tenaga listrik dalam *real time operation* seperti frekuensi, tegangan, daya aktif dan daya reaktif, serta *tap changer position* dapat dikirimkan ke *control centre* atau pusat pengatur beban melalui sarana teleinformasi yang disebut telemetering.

Dengan demikian maka secara prioritas fungsi teknologi informasi SCADA adalah sebagai berikut :

**1. Telemetering**

Telemetering adalah proses pengambilan besaran ukur tenaga listrik yang ada di gardu induk atau pusat pembangkit yang dapat dimonitor di *control center*.

**2. Telesignalling**

Status dari peralatan tenaga listrik, sinyal alarm dan sinyal lainnya yang ditampilkan disebut status indikasi. Status indikasi terhubung ke modul digital input. Status indikasi terdiri dari indikasi tunggal (*single*) dan indikasi ganda (*double*). Indikasi ganda terpasang pada peralatan yang mempunyai dua keadaan, dimana satu keadaan menunjukan kontak terbuka (*open*) dan satu lain kontak tertutup (*close*), seperti pada PMT (Sakelar Pemustus Tenaga/*Circuit Breaker*)dan PMS (Sakelar Pemisah/*Disconect Switch*) . Indikasi tunggal dipergunakan untuk menyampaikan data alarm dari peralatan tenaga listrik. Status indikasi dikirim ke pusat pengatur beban bila terjadi perubahan status dari peralatan.

**3. Fungsi Kontrol**

Fungsi kontrol sistem tenaga listrik terbagi menjadi 4 bagian, yaitu:

a) Kontrol individu, kontrol perintah untuk pengaturan peralatan, pola kontrol otomatis dan pola kontrol berurutan.
b) Kontrol individu, merupakan perintah langsung ke peralatan sistem tenaga listrik, seperti perintah tutup/buka PMT atau PMS, perintah *start* atau *stop* unit pembangkit.
c) Kontrol perintah untuk menaikkan atau menurunkan daya pembangkitan.

**Metode Penelitian**

Hubungan Teknologi Informasi pada SCADA, resiko adalah dampak yang ditimbulkan atas terjadinya sesuatu yang mengancam Keamanan Teknologi Informasi SCADA di PLN. Guna menentukan kemungkinan terjadinya peristiwa yang merugikan di masa yang akan datang, ancaman terhadap sistem TI SCADA harus dianalisis dan dihubungkannya dengan kerentanan (*vulnerlibility*) potensial dan kontrol keamanan di tempat Teknologi Informasi SCADA di APB XXX. Untuk menjawab rumusan masalah dan menguji hipotesis di perlukan metode penelitian dengan cara survey.

Tahapan-tahapan yang harus dilakukan untuk menilai resiko Teknologi Informasi SCADA adalah sebagai berikut ;

1) Melakukan studi perpustakaan

Pada tahap ini dilakukan kajian pustaka dan referensi yang menunjang teori-teori bidang Resiko Keamanan pada SCADA serta metodologinya. Juga disertai

penelitian-penelitian terdahulu dan hal-hal empiris.

2) Menentukan desain penelitian

Pada bagian ini mengikuti desain penelitian untuk menilai resiko dengan tahapan seperti tercantum dalam NIST SP 800-30 sebagai rujukan dari NIST SP 800-82 (Guide to Industrial Control System (ICS) Security. Yang meliputi menentuka karakeristik sistem, identifikasi serangan, identifikasi kerentanan, analisa kontrol, menentukan kemungkinan, analisa dampak, menentukan resiko, rekomendasi kontrol, dokumentasi hasil.

3) Menyususn instrumen dan mengumpulkan data

Pada bagain ini Instrumen yang digunakan adalah NIST SP 800-82 yang didalamnya merujuk kontrol keamanan berdasarkan NIST SP 800-53 (Assessment and Authorizen (CA) yang selanjutnya dijabarkan dalam pertanyaan-pertanyaan indikator, sedangkan dalam pelaksaan pengumpulan data nilao objektivitas dan keakuratan data yang diperoleh tetap memenuhi aturan dan keetisan tetap diperhatikan.

4) Menganalisis data dan menyajikan hasil

Pada bagian ini akan dijelaskan teknik dan langkah-langkah yang ditempuh untuk menganalisis atau mengolah data. Karena menggunakan data kuantitatif maka akan dianalisis dengan teknik statistik deskriftif, yang akan ditampilkan berupa grafik, profil, atau bagan.

5) Mengiterprestasikan hasil temuan serta membuat kesimpulan dan saran

Bagian ini hasil analisis data akan ditafsirkan dengan meliat makna hubungan antara temuan yang satu dan yang lainnya, antara temuan dan latar belakang dengan kemungkinan penerapannya.

## Hasil dan Pembahasan

### A. Analisa Data

Dari hasil pengumpulan data didapat kerentanan pada aset-aset APB XXX .

1) Penilaian Resiko dan Ancaman pada Aset Perangkat Keras dan Sistem Operasi pada Master Station sistem SCADA.
2) Penilaian Resiko dan Ancaman pada aset Aplikasi Perangkat Lunak di Master Station sistem SCADA.
3) Penilaian Resiko dan Ancaman pada Aset Jaringan pada sistem SCADA

4) Penilaian Resiko dan Ancaman pada Aset Sumber Daya Manusia di sistem SCADA
5) Penilaian Resiko dan Ancaman pada Aset Gedung dan Lingkungan dimana sistem SCADA berada.
6) Penilaian Resiko dan Ancaman pada Aset Kendali Management dan Umpan Balik di sistem SCADA.
7) Penilaian Resiko dan Ancaman pada Aset Manajemen Informasi yang terkait sistem SCADA
8) Penilaian Resiko dan Ancaman pada Utilitas Pendukung sistem SCADA.

Identifikasi Kerawanan adalah bagian dari tabel-tabel Penilaian Ancaman dan Resiko pada Aset Master Station SCADA APB XXX. ahap-tahap dalam menentukan analisis Resiko dalam NIST SP 800 30 adalah :

1) Menetapkan kontrol-kontrol yang saat ini berjalan
2) Merencanakan kontrol-kontrol yang akan dilakukan

Hasil dari langkah tersebut adalah berupa matrik kontrol saat ini dan yang direncanakan, yang diberikan pada tabel 3.

**Tabel 3.**

| Kemungkinan | |
|---|---|
| Jarang | Probabilitas kemungkinan terjadi rendah 0 – 5 kali pertahun |
| Sedang | Probabilitas kemungkinan terjadi sedang 6 – 10 kali pertahun |
| Sering | Probabilitas kemungkinan terjadi tinggi > 10 kali pertahun |

Langkah berikutnya dalam mengukur tingkat resiko adalah menentukan dampak merugikan akibat suksenya ancaman bagi sebuah kerentanan. Sebelum memulai analisis dampak dikumpulkan dahulu informasi-informasi hal dibawah ini:

1) Misi sistem
2) Sistem dan data sistem dan kritisnya
3) Sistem dan kesensitipan data

Nilai keritisan sebuah aset menginformasi identifikasi dan prioritas bagi APB berdasarkan penilaian kwalitas dan kuntitas. Selain itu dihubungkan dengan

tujuan CIA atau Integrity (integritas), availability (ketersedian) dan Convidentiality (kerahasian). Dirangkum dalam tabel definisi dibawah ini :

**Tabel 4. Nilai Kritikal**

| | **Dampak** |
|---|---|
| Rendah | Dampak tidak penting bagi APB<br>Dampak tidak terlalu berpengaruh pada APB<br>Down time sistem SCADA rendah ≤ 60 menit |
| Sedang | Dampak berpengaruh pada kegiatan operasional APB<br>Nilai kerusakan penting bagi APB<br>Down time sistem SCADA sedang adalah ≤ 120 menit |
| Tinggi | Dampak berpengaruh pada operasional dan bisnis APB<br>Nilai kerusakan menjadi perhatian utama APB<br>Downtime lebih dari ≥120 menit |

Tujuan dari langkah ini adalah untuk menilai tingkat risiko untuk sistem SCADA APB. Penentuan nilai risiko pasangan ancaman/kerentanan tertentu dinyatakan sebagai :

1) Kemungkinan diberikan oleh sumber-ancaman ini mencoba kerentanan yang ada
2) Besarnya dampak dari sumber-ancaman jika berhasil melaksanakan kerentanan
3) Kecukupan kontrol keamanan yang direncanakan atau yang ada untuk mengurangi atau menghilangkan resiko.

**Tabel 5. Nilai Ancaman terhadap Dampak**

| **Kemungkinan Ancaman** | **Dampak** | | |
|---|---|---|---|
| | **Rendah (10)** | **Sedang (50)** | **Tinggi (100)** |
| Tinggi (1.0) | 10 X 1,0 = 10<br>Rendah | 50 X 1,0 = 50<br>Sedang | 100 X 1,0 = 100<br>Tinggi |
| Sedang (0.5) | 10 x 0,5 = 5<br>Rendah | 50 X 0,5 = 25<br>Sedang | 100 X 0,5 = 50<br>Sedang |
| Rendah (0.1) | 10 X 0,11 = 1<br>Rendah | 50 X 0,1 = 5<br>Rendah | 100 X 0,1 = 10<br>Rendah |

**Skala Resiko dan Aksi yang diperlukan**

**Tabel 6. Skala Resiko**

| Tingkat Resiko | Penjelasan Resiko dan Aksi yang diperlukan |
|---|---|
| Tinggi | Hasil observasi atau temuan dievaluasi beresiko tinggi, dan mempengaruhi kegiatan operasional, bisnis dan keselamatan APB. Sistem sekarang boleh melanjutkan operasi , tetapi rencana aksi koreksi harus dimasukan segera dan nyata. |
| Sedang | Hasil observasi atau temuan dievaluasi beresiko sedang, mempengaruhi kegitan operasional dan bisnis APB. Tindakan perbaikan diperlukan dan rencana harus dikembangkan selanjutnya dimasukan ke dalam tindakan dengan periode waktu yang wajar. |
| Rendah | Hasil observasi adalah menggambarkan beresiko rendah, tidak berpengaruh terhadap operasional, bisnis dan keselamatan APB. Sistem harus menentukan apakah tindakan perbaikan diperlukan atau memutuskan menerima resiko. |

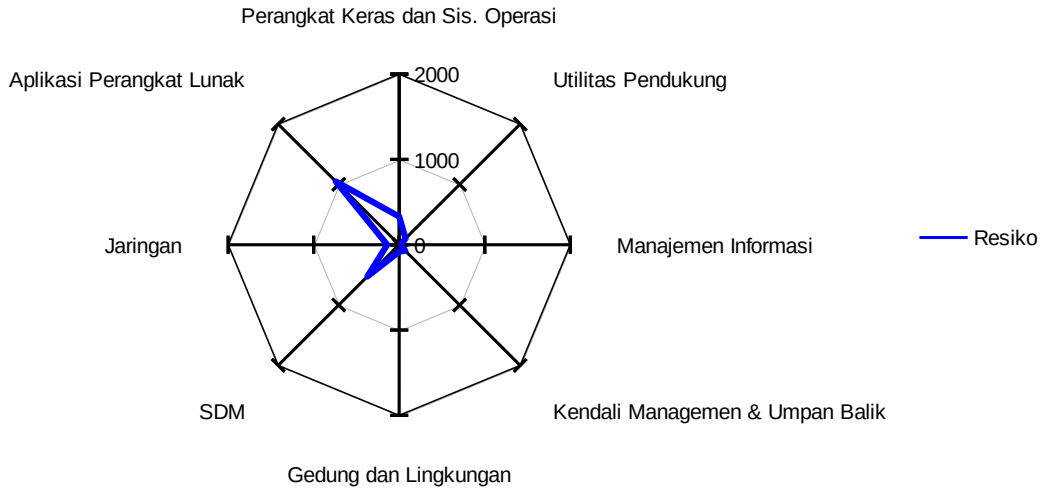
Selanjutnya dibuat matrik Penilaian Ancaman dan Resiko pada :

1). Aset Perangkat Keras dan Sistem Operasi pada Master Station APB XXX
2) Aset Aplikasi Perangkat Lunak di Master Station
3) Aset Jaringan di APB XXX
4) Aset Sumber Daya Manusia di APB XXX
5) Aset Gedung dan Lingkungan
6) Aset Kendali Management dan Umpan Balik
7) Aset Manajemen Informasi
8) Aset Utilitas Pendukung

**B. Rekomendasi Kontrol**

Dari hasil wawancara, observasi terhadap aset-aset yang ada pada Sistem SCADA, maka dilakukan pembuat chart penilaian resiko kemanan yang hasilnya adalah seperti dibawah ini.

**Gambar 2. Chart penilaian resiko kemanan pada Sistem SCADA APB XXX**




Setelah mengetahui resiko-resiko yang dihadapi oleh Aset SCADA, maka selanjutnya dipilih kontrol yang akan digunakan sebagai digunakan untuk mengurangi resiko. Untuk menetapkan control dapat dilihat kerawanan, ancaman dan dampak. Seperti pada tabel 7 Rekomendasi dan kontrol yang harus dilakukan.

| Ref | Objek Kontrol | Pemilihan kontrol untuk mencapai tujuan | Resiko Terkontrol | | Resiko yang Tersisa |
|---|---|---|---|---|---|
| | | | Konsekwensi | Kemungkinan | |
| RP 1 Aset Sumber Daya Manusia (Confidentiality) | Untuk memastikan bahwa orang menjaga kerahasiaan informasi SCADA yang sensitif | Perjanjian Rahasia Pekerjaan dalam kontrak kerja. (NIST SP 800-53 Rev. 4 CP - 2) | Rendah | Rendah | Diterima |
| RP 2 SDM (Integrity) | Untuk memastikan bahwa sumber daya SCADA dilatih dengan tepat, termotivasi dan dapat dipercaya | Uraian pekerjaan harus ringkas dan jelas dalam Bahasa Indonesia (NIST 800-53 Rev 4 AT -2, PM-13. | Rendah | Rendah | Diterima |
| RP 5 Kontrol Manajemen & Umpan Balik (Integrity) | Untuk memberikan akses yang benar dan terkendali ke informasi SCADA | Repositori terkendali untuk informasi terkait SCADA. Sistem manajemen informasi / pengetahuan dapat membantu mencapai penyimpanan yang terkendali dan aman - ( NIST SP 800 53 Rev. 4 MP-8, SC-12, SC-28)). | Rendah | Rendah | Diterima |
| | Untuk memberikan respon insiden dan proses kesiapan | Kesiapan forensik adalah kemampuan organisasi untuk memaksimalkan kemampuan pengumpulan bukti sambil meminimalkan biaya untuk melakukannya. ( NIST SP 800 53 Rev. 4 AU-7, IR-4)) | Rendah | Rendah | Diterima |
| RP 6 | Untuk memastikan | Peran dan Tanggung Jawab untuk Manajemen | Rendah | Rendah | Diterima |

| | | | | | |
|---|---|---|---|---|---|
| Kontrol Manajemen & Umpan Balik (Availability) | bahwa kontrol manajemen yang diperlukan ditentukan | yang disetujui dan didokumentasikan (NIST SP800-53 Rev. 4 -1 Pengendalian dari semua acuan kendali keamanan ) | | | |
| | Untuk memberikan dukungan Manajemen yang berdedikasi dan efektif untuk sistem SCADA Didokumentasikan | Kebijakan dan prosedur manajemen SCADA yang terdokumentasi Dokumen ini harus singkat dan tidak berubah secara signifikan dari waktu ke waktu ( NIST SP800-53 Rev. 4 -1 ) | Rendah | Rendah | Diterima |
| RP 9 Building / Site (Availability) | Untuk mencegah hilangnya aset dan gangguan pada operasi SCADA | Batas keamanan yang ditentukan Membatasi akses ke situs - jangan izinkan akses luas hanya untuk kenyamanan ( NIST SP 800-53 Rev. 4 AT-3, IR-2, PM-13 ) | Rendah | Rendah | Diterima |
| RP 10 Manajemen Informasi (Confidentiality ) | Untuk mengontrol akses ke informasi SCADA | Kebijakan kontrol akses SCADA yang terdokumentasi Kebijakan akses tingkat tinggi harus menjadi bagian dari kontrol manajemen informasi yang dikomunikasikan kepada manajemen dan pengguna ( NIST SP800-53 Rev. 4 AC-1, AC-2, AC-3, AC-5, AC-6, AC-14, AC-16, AC-24) | Rendah | Rendah | Diterima |
| RP 10 Manajemen Informasi ( | Untuk memastikan operasi yang benar dari fasilitas pemrosesan informasi maka didokumentasikan | Prosedur operasi SCADA yang terdokumentasi Agar memiliki efek penuh; prosedur operasi harus konsisten, tersedia, jelas dan perubahan harus diterapkan secara efisien sesuai dengan kontrol versi yang tepat. | Rendah | Rendah | Diterima |

| | | | | | |
|---|---|---|---|---|---|
| Integrity) | | ( NIST SP800-53 Rev. 4 Semua keluarga kendali keamanan ) | | | |
| RP 12 Komunikasi & Jaringan (Availability ) | Untuk menjaga konektivitas jaringan SCADA | Untuk layanan utama, rute jalur komunikasi melalui beberapa media. ( NIST SP800-53 Rev. 4 ) | Rendah | Rendah | Diterima |
| RP 13 Aplikasi perangkat lunak SCADA (Confidentiality ) | Untuk memastikan bahwa perangkat lunak tersebut menggunakan mekanisme keamanan praktik terbaik yang diakui dan mampu menahan upaya akses yang tidak sah. | Konfigurasi perangkat lunak SCADA yang aman Jika memungkinkan, sistem yang terkomputerisasi harus diperkeras untuk meminimalkan peluang akses yang tidak sah. Pengerasan juga harus memastikan bahwa setiap dukungan perangkat lunak aplikasi vendor dipertahankan sepanjang umur produk sementara sistem yang mendasarinya hardering. Mekanisme kontrol akses juga harus ada untuk memastikan bahwa kontrol akses sistem terpusat dilindungi sesuai dengan kata sandi perusahaan dan kebijakan penggunaan akun. (NIST SP 800 -53 rev. 4 SA – 9, SA – 11, SA -12, PM -9) | Rendah | Rendah | Diterima |
| RP 13 Aplikasi perangkat lunak SCADA (Integrity ) | Untuk menjaga pengoperasian perangkat lunak yang benar dari waktu ke waktu | Menerapkan proses manajemen Improving - Manajemen kerentanan teknis, ISM - Manajemen Kerentanan) NIST SP 800 53 Rev. 4 CP 2, IR – 4, IR - 8 | Rendah | Rendah | Diterima |

| | | | | | |
|---|---|---|---|---|---|
| RP 14 SCADA Hardware including operating System (Confidentiality ) | Untuk memastikan bahwa platform komputasi SCADA tangguh terhadap upaya akses yang tidak sah | Hardering keamanan platform komputasi, Platform komputer harus diperkeras untuk menghapus layanan, akun, dan paket perangkat lunak yang tidak perlu. Perjanjian dukungan vendor harus memungkinkan pengerasan dasar platform komputer yang didukung. ( NIST 800 53 Rev 4, CP -2, RA-2, SA-14, SC - 6) | Rendah | Rendah | Diterima |
| RP 15 SCADA Hardware including operating System (Integrity ) | Untuk memastikan bahwa konfigurasi platform komputasi SCADA dalam kondisi yang diketahui dan disetujui. | Manajemen konfigurasi formal dan prosedur kontrol. Harus ada langkah-langkah yang berlaku untuk memastikan bahwa sistem SCADA berada dalam kondisi yang diketahui dan disetujui, dan bahwa perubahan dianalisis, diuji, dan disahkan dengan tepat. (NIST SP 800 – 53 Rev. 4 MA – 2, MA – 3, MA – 5, MA -6) | Rendah | Rendah | Diterima |
| RP 16 SCADA Hardware including operating System (Availability) | Untuk memastikan bahwa platform komputasi SCADA dapat diandalkan jika terjadi kerusakan komponen, gangguan lingkungan, atau upaya gangguan berbahaya | Redundansi sistem Komponen sistem kritis harus dirancang untuk menahan titik kegagalan tunggal. Rencana Kesinambungan Bisnis (dan / atau jika perlu, Rencana Pemulihan Bencana) harus diperbarui dan diuji untuk memastikan bahwa sistem dapat menahan hilangnya ketergantungan fisik, personel, dan prosedural tunggal. (NIST 800 53 Rev 4 CP -2, IR -4, IR-8) | Rendah | Rendah | Diterima |
| RP 17 Supporting Utilities Confidentiality | Untuk memastikan bahwa kegagalan daya tidak mengarah pada gangguan keamanan sistem SCADA | Sumber daya cadangan Komponen sistem yang kritis harus diumpankan melalui catu daya utama dan cadangan. (NIST 800 53 REV. 4, CP-2, RA-2, SA-14, SC-6) | Rendah | Rendah | Diterima |

| | | | | | |
|---|---|---|---|---|---|
| RP 18 Supporting Utilities (Integrity | Untuk memastikan bahwa sistem SCADA beroperasi seperti yang diharapkan selama gangguan pasokan daya | Sumber daya cadangan Cadangan alternatif catu daya Jangka menengah hingga panjang (seperti unit daya diesel jangka panjang) harus tersedia untuk memberi daya pada komponen sistem SCADA yang kritis selama gangguan daya. Jika komponen inti SCADA dipasang di lingkungan kontrol khusus, catu daya juga harus mampu memberi daya pada lingkungan pendukung seperti pendingin udara dan deteksi kebakaran. ( NIST 800 53 REV. 4, CP-2, RA-2, SA-14, SC-6) ) | Rendah | Rendah | Diterima |
| RP 19 Supporting Utilities ( Availability ) | Untuk mencegah gangguan pada operasi SCADA selama kondisi kegagalan daya | Pengujian pemulihan bencana Rencana darurat harus diuji secara berkala. Apabila tes kegagalan fisik tidak dapat dilakukan, pengujian skenario formal harus dilakukan, dengan hasil dan pelajaran yang diperoleh didokumentasikan, dianalisis, dan ditindaklanjuti sebagaimana mestinya. ((NIST 800 53 Rev. 4 CP-4, IR-3, PM-14 ) | Sedang | Sedang | Diteruskan |

**Kesimpulan**

Dari paparan hasil penilaian resiko yang sudah dilakuakan perbaikan menuju keamanan infrastruktur kritis khususnya di APB, ada beberapa kesimpulan kerentatanan yang dihadapi oleh sistem SCADA APB :

1. Masih bergantungnya aplikasi SCADA terhadap pihak ke tiga yang rentan disalah gunakan pihak yang menginginkan penguasaan terhadap sistem kendali industri untuk hajat hidup WNI.
2. Masih lemahnya kesadaran pengamanan hak akses dan pelatihan pengamanan yang harus dimonitor secara berkala.
3. Masih adanya piihak ketiga sebagai pengembang aplikasi dan perangkat keras yang rentan untuk kontinuitas dukungannya.
4. Belum adanya redudansi jaringan keluar yang terhubung dengan piranti scada lapangan menyebabkan rentas jika ada gangguan.
5. Belum redudansinya perangkat sistem SCADA untuk APB yang rentan jika ada gangguan pada salah satu bagian.
6. Sumber daya manusia yang mengusai dan mengoperasikan SCADA sangat terbatas rentan jika ada masalah dengan SDM yang ada.
7. Lokasi ruang mastering SCADA ada di gedung yang rentan terkena bencana alam.
8. Kendali Management dan Umpan Balik mempunyai kerentatan karena belum adanya komite keamanan yang membuat kebijakan keamanan.
9. Manajemen Informasi masih rentan dengan kebocoran informasi SCADA .
10. Utilitas Pendukung masih rentan ketika dibutuhkan dukungan ketika kehilangan sumber daya utama.

## BIBLIOGRAFI

BPPT, PTPSE. 2014. *Outlook Energi Indonesia 2014*. E-Pustaka: Jakarta.

US. Departmen of Commerce, NIST, NIST SP800-82 Guide to Industrial Control System (ICS) security, Gaithersburg, 2015

http://perpustakaan.bappenas.go.id/lontar/file?file=digital/blob/F7089/Listrik%20Padam-MI.htm, Listrik Padam-Kerugian mencapai miliaran rupiah, Media Indonesia, 19 agustus 2005.

http://perpustakaan.bappenas.go.id/lontar/file?file=digital/blob/F30984/Sistem%20Kelistrikan%20Jawa.htm, Sistem Kelitrikan Jawa Bali riskan-Sistem tranmisi Satu dan sudah tua, Kompas, 18 agustus 2005.

US. Departmen of commerce, NIST, NIST SP 800-30- Computer security-Risk Management Guide for Information technology System, July 2002.

US. Departmen of commerce, NIST, NIST SP 800-53A- Assessing Security and Privacy Control in Federal Information System and Organizations- Building Effective Assessment Plans, Desember 2014.

US. Departmen of commerce, NIST, NIST SP 800-37 Rev 1- Guide for Applying the Risk Management Framework to Federal Information Systems-Security Life Cycle approach, Februari 2010.

Stouffer Keith , NIST Briefing: ICS Cybersecurity Guidance – NIST SP 800-82, Guide to ICS Security, 28 Agustus 2013.

NIST, Framework for Improving Critical Infrastructur Cybersecurity – versi 1, Februari 2014.

Chipley Michael, Cybersecuring DoD Industrial Control Systems, Maret 2014.

Wahidah Rohimatul. Tata Kelola Keamanan Informasi pada Area Transmisi PT. PLN (Persero) P3B Jawa Bali menggunakan Cobit 5 dan ISO/IEC 27001:2013, STEI ITB, 2014.

Wilhoit Kyle, ICS_SCADA and Non-traditional Incident Response,-Trend Micro, 2014

IT Security Expert advisory Group (ITSEAG), Generic SCADA Risk Management Framework for Australian Critical Infrastructure , Maret 2012

Sarno Riyanarto, Sistem Keamanan Sistem Informasi- Teori, Perancangan dan Implementasi berbasis ISO 27001, ITS Publisher, 2012

Roodhin Firmana; Bekti Cahyo Hidayanto, S.Si, M.Kom; Hanim Maria Astuti, S.Kom, M.Sc, TIK - PT.PLN DISTRIBUSI JATIM dengan Indeks Kami dan ISO 27001, 2013

Rizki Komalasari, Ilham Perdana, Audit Keamanan Informasi bagian teknologi informasi PT PLN DJBB, 2009

Prasetio Joko, Workshop Scada Nasional- Review SPLN 109: Pola Scada dan Oveview IEC 879: Telecontrol, 10-2004

PT. PLN, Grand design Teknologi Informasi, Surabaya, 2012

Terezinho Fabio, White paper-SCADA System automate Electrical Distribution, Indusoft, http://www.automation.com/pdf_articles/SCADA_white_paper.pdf.

Igor Nair Fovino, Marcelo Masera, Rafal Leszczyna, Joint Research – ICT Security Assessment of a Power Plant, a case Study, https://www.viestintavirasto.fi/attachments/hvk-materiaali/automaatio/5llafcpkp/power_plant_risk2-2.pdf Majalah Gedung Miring, Komunikasi Radio Riwayatmu Kini-Paparan Gangguan Sub_Sistem Jawa tengah- 3 September 2013-Dari Sudut.