Makalah Tugas Kuliah EL6115
Operasi Keamanan dan *Incident Handling*

RESPON INSIDEN UNTUK KEAMANAN INFORMASI *PHASOR MEASUREMENT UNIT* PADA *SMART GRID*

Oleh :

RAMADHANI ULFITA IZANTARI N.
23215118

Dosen :

Dr. Ir. Budi Rahardjo

SEKOLAH TEKNIK ELEKTRO DAN INFORMATIKA
PROGRAM MAGISTER TEKNIK ELEKTRO
INSTITUT TEKNOLOGI BANDUNG

2015

ABSTRAK

Smart grid merupakan sebuah *grid* modern yang dapat mengalirkan energi secara dua arah, menggunakan komunikasi dua arah dan kemampuan kontrol yang akan menimbulkan fungsionalitas dan aplikasi baru. Salah satu komponen terpenting dari *smart grid* adalah sistem teknologi komunikasi dan informasi yang memiliki peran penting dalam mengoperasikan, mengatur, merencanakan, dan mengamankan infrastruktur energi dari proses pembangkitan, transmisi, distribusi, dan konsumsi. Salah satu perangkat yang berperan penting dalam sistem transmisi pada *smart grid* adalah *Phasor Measurement Unit* (PMU). PMU adalah sebuah perangkat yang menghasilkan nilai fasor, frekuensi, dan laju perubahan frekuensi tersinkronisasi dari sinyal tegangan dan/atau arus dan sebuah sinyal pensinkronisasi waktu.

Fitur tepenting dari teknologi PMU adalah hasil pengukuran *Wide Area Monitoring System* (WAMS) di suatu sumber dilengkapi dengan *time stamp* dengan presisi yang tinggi yang dihasilkan dari GPS. Hasil pengukuran PMU dengan *time stamp* digunakan untuk merujuk pada kondisi sistem tenaga tepat pada waktu yang didefinisikan oleh *time stamp*. PMU melakukan komunikasi dengan *Phasor Data Concentrator* (PDC). Sistem kerja PMU rentan terhadap terjadinya insiden yang bertujuan untuk mengganggu ketersediaan layanan pengukuran dan memodifikasi data hasil pengukuran yang ditransmisikan. Respon insiden pada PMU dibutuhkan untuk meminimalisasi meluasnya dampak insiden dan mengembalikan sistem PMU beroperasi normal kembali.

Dalam makalah ini, disusun suatu model baru dalam menghadapi insiden yang terdiri dari rangkaian kegiatan pra-insiden yang meliputi penyusunan kebijakan dan prosedur, pembagian peran dan tanggung jawab, pelatihan, dan pengujian respon insiden sebagai persiapan dalam menghadapi insiden. Kemudian dirancang rangkaian kegiatan saat terjadinya insiden yang meliputi deteksi, koordinasi respon darurat, investigasi dan analisis respon insiden, dan tindakan korektif. Pasca terjadinya insiden, dilakukan pelaporan insiden dan resolusi.

Kata kunci: model respon insiden, *smart grid*, PMU

DAFTAR ISI

BAB I PENDAHULUAN

Ketersediaan layanan listrik merupakan salah satu kebutuhan dasar dari masa modernisasi saat ini. Peningkatan perhatian terhadap aspek energi dan lingkungan turutmendorong peningkatan permintaan terhadap sistem kelistrikan yang dapat diandalkan, efisien, dan ramah lingkungan. *Smart grid* merupakan sebuah sistem yang tepat untuk memenuhi kebutuhan tersebut. *Smart grid* merupakan sebuah grid modern yang dapat mengalirkan energi secara dua arah, yang menggunakan komunikasi dua arah dan kemampuan kontrol yang akan menimbulkan fungsionalitas dan aplikasi baru [1]. *Smart grid* menjalankan fungsi sensor, pengawasan, komunikasi, otomasi, dan komputer untuk meningkatkan fleksibilitas, keamanan, reliabilitas, efisiensi, dan keamanan dalam sistem kelistrikan. Salah satu komponen terpenting dari *Smart grid* adalah sistem teknologi komunikasi dan informasi yang berperan penting dalam mengoperasikan, mengatur, merencanakan, dan mengamankan infrastruktur energi dari proses pembangkitan, distribusi, dan konsumsi energi. Peran dari sistem teknologi komunikasi dan informasi dalam *smart grid* di antaranya untuk melakukan komunikasi data, pemodelan sistem, dan pengamanan data. Seiring dengan peningkatan penggunaan teknologi komunikasi dan informasi, tantangan yang harus dihadapi juga meningkat, di antaranya dalam hal keamanan, privasi, timing, fungsionalitas yang bersifat *real time*, dsb [2].

Salah satu perangkat terpenting dalam sistem transmisi *smart grid* adalah PMU yang berfungsi mengukur gelombang listrik menggunakan sebuah sumber *common time* untuk melakukan sinkronisasi untuk memungkinkan dilakukannya pengukuran *real time* tersinkronikasi dari berbagai titik pengukuran dalam suatu *power grid* [1]. Hasil pengukuran PMU dapat digunakan untuk menganalisis terjadinya ketidakstabilan pada sistem. PMU membutuhkan hubungan komunikasi untuk melakukan pengiriman data hasil pengukuran berupa arus, tegangan, frekuensi, dan laju

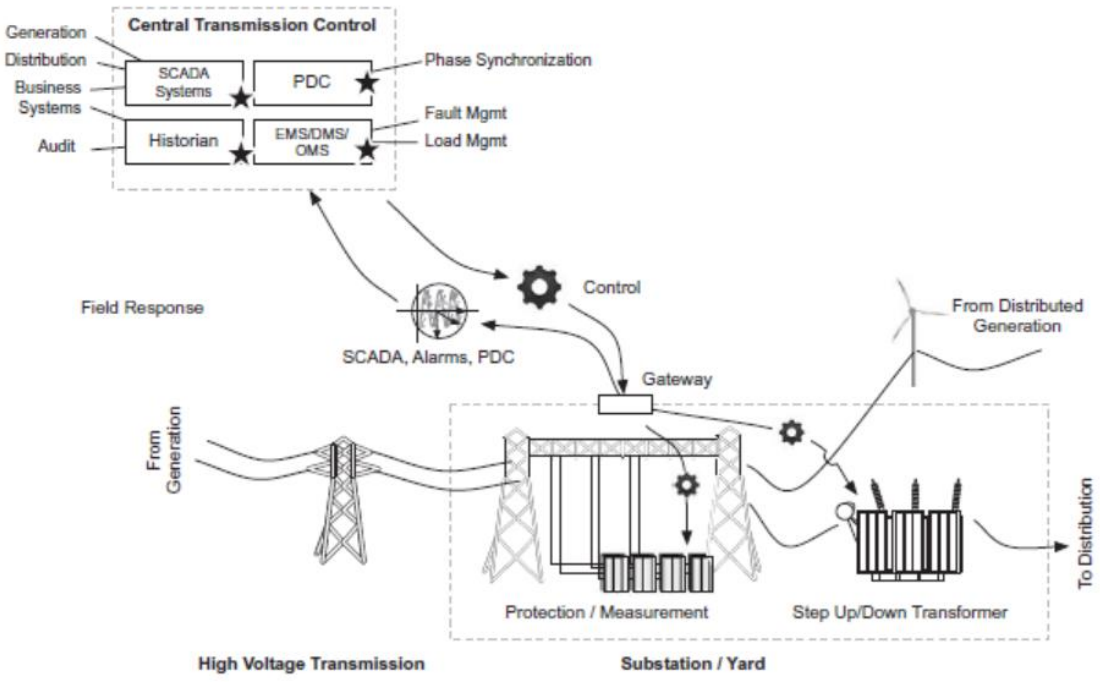
perubahan frekuensi beserta time-stamp untuk setiap nilai parameter yang diukur dari suatu bagian sistem tenaga ke perangkat. Data hasil pengukuran PMU dikirimkan ke perangkat dengan tingkat hirarki yang lebih tinggi untuk dapat digunakan dalam menjalankan tugas suatu aplikasi. Selain mengirim data, PMU juga dapat menerima perintah dari perangkat yang lebih tinggi melalui hubungan komunikasi [3]. Data yang dikirim dan diterima PMU tersebut merupakan data sensitif yang hanya dapat diakses oleh orang yang memiliki otorisasi yang legitimate. Hal ini dikarenakan data yang dihasilkan oleh PMU mengacu kepada keadaan suatu *power grid* sesuai dengan waktu yang didefinisikan dalam *time stamp* yang berfungsi untuk menjalankan berbagai aplikasi pengawasan, pengendalian, dan perlindungan pada suatu wilayah *power grid* [4]. Sehingga, insiden yang berisiko menyebabkan kerusakan, kehilangan, dan perubahan konten data dapat mempengaruhi kinerja aplikasi yang berfungsi mengontrol fungsionalitas sistem tenaga.

Oleh karena itu, dibutuhkan suatu pemodelan sistem insiden untuk mempersiapkan suatu organisasi dalam menghadapi insiden, melakukan penanganan insiden yang tepat, dan mempersiapkan laporan dan resolusi untuk persiapan respon insiden yang akan datang.

BAB II TINJAUAN PUSTAKA

2.1 Sistem Transmisi pada *Smart Grid*

Setelah energi dibangkitkan, energi ditransmisikan kepada titik-titik distribusi untuk kemudian disampaikan pada *end user*. Sistem transmisi membutuhkan teknologi komunikasi pada wilayah *power grid* yang luas untuk mendukung infrastruktur pengukuran *real time*, dan membutuhkan sistem *Supervisory Control and Data Acquisition* (SCADA) untuk menjalankan automasi operasi *real time*. Gardu merupakan komponen primer dalam sistem transmisi. Gardu berfungsi menjalankan pengukuran tegangan, pengaturan tegangan, dan perlindungan line sehingga listrik dapat ditransmisikan secara aman dan efisien.



Gambar II-1 Arsitektur Sistem Transmisi [5]

Modernisasi pada sistem transmisi berfokus pada penambahan inteligensi dan otomasi untuk membuat transmisi energi lebih efisien (melalui optimasi *grid* seperti beban dinamis dan manjemen kondisi), lebih dapat dihandalkan (melalui ketahanan terhadap serangan dan kemampuan memulihkan diri), dan lebih fleksibel (mendukung pembangkitan terdistribusi). Penggunaan sistem teknologi pada sistem transmisi *smart grid* yang bertujuan mengakomodasi sistem transmisi yang lebih cerdas turut diiringi dengan munculnya tantangan terhadap keamanan siber. Berdasarkan Gambar II-1, komponen penyusun sistem transmisi terdiri dari otomasi gardu, GPS/*satelite timing*, sistem pengukuran wilayah luas, dan perlindungan dan kontrol lanjutan, yang ketika dikombinasikan dengan pengendali terdistribusi dan sistem SCADA akan menyebabkan berbagai ancaman siber terhadap sistem transmisi. Beberapa sasaran dalam infrastruktur transmisi di antaranya adalah sebagai berikut [5].

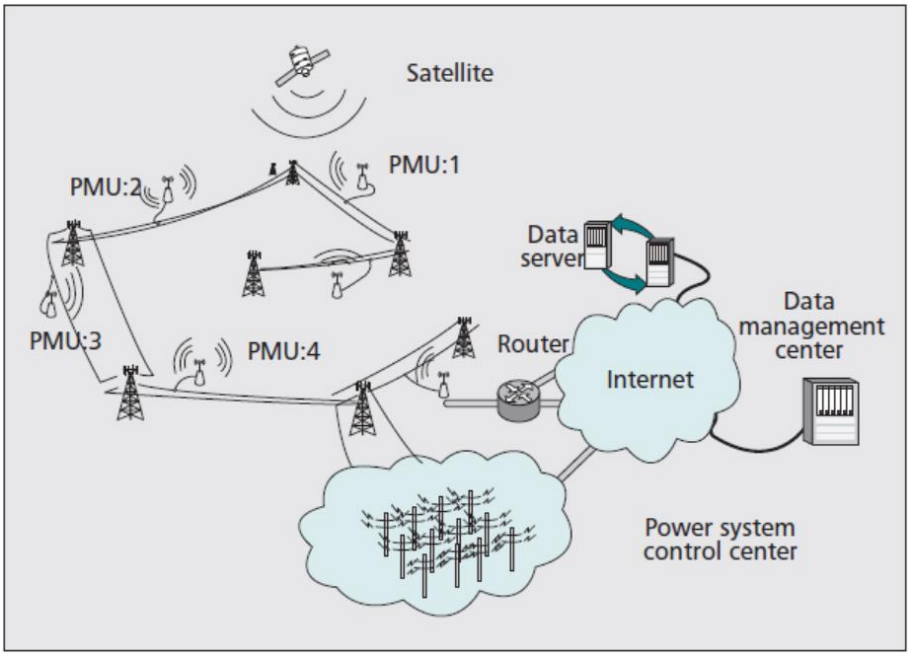
- Transmisi SCADA dan sistem otomasi gardu.
- Sistem pengukuran fasa pada PMU.
- Sistem perlindungan line untuk mencegah lonjakan dan pemadaman.
- Transformer yang digunakan untuk membentuk listrik untuk dapat memenuhi tegangan utransmisi yang efisien dan aman.

2.2 *Wide Area Monitoring, Protection and Control System (WAMPAC)*

Sistem Wide Area Monitoring, Protection and Control (WAMPAC) membutuhkan PMU untuk menghasilkan pengukuran yang digunakan untuk melakukan pengawasan *real time* terhadap operasi suatu *grid* dan juga menyediakan perlindungan *real time* serta fungsi kontrol seperti *Special Protection Schemes* (SPS) dan *Automatic Generation Control* (AGC). Hasil pengukuran dari PMU digunakan dalam aplikasi lainnya seperti deteksi osilasi, dan prediksi stabilitas transien. Komunikasi merupakan kunci untuk *smarter grid*, sehingga mengembangkan dan mengamankan infrastruktur siber dan protokol komunikasi merupakan hal yang penting. WAMPAC dapat dibagi ke dalam beberapa komponen penyusunnya, yaitu

Wide-Area Monitoring System (WAMS), *Wide-Area Protection Systems* (WAP), dan *Wide-Area Control* (WAC).

PMU menggunakan laju pencuplikan yang tinggi dan sistem waktu yang akurat berdasarkan GPS sesuai dengan gambar II-2 untuk menyediakan pembacaan *grid* yang tersinkronisasi dengan tingkat akurasi yang tinggi. Perkembangan aplikasi kendali lanjut tergantung pada pada efektivitas WAMS dalam mendistribusikan informasi secara aman dan handal.



Gambar II-2 Arsitektur WAMS [6]

WAP meliputi penggunaan sistem pengumpulan informasi dalam lingkup wilayah yang luas untuk melakukan pengambilan keputusan secara tepat mengenai tindakan yang harus dilakukan untuk mengatasi propagasi suatu gangguan [7]. Perkembangan PMU telah mengubah sistem perlindungan dari konsep lokal menjadi konsep sebuah sistem dengan wilayah cakupan yang luas untuk mengatasi gangguan. Salah satu aplikasi yang umum digunakan dalam WAP adalah SPS, yaitu sistem perlindungan

otomatis yang dirancang untuk mendeteksi kondisi sistem yang tidak normal dan tidak terdefinisikan sebelumnya, dan melakukan tindakan koreksi untuk mengisolasi kegagalan komponen dala memelihara kehandalan sistem. Tindakan tersebut melliputi perubahan dalam pembangkitan (MW dan MVAR), atau konfigurasi sistem untuk memelihara stabilitas sistem, tegangan yang dapat diterima, atau aliran daya.

Mekanisme WAC dalam *power grid* adalah AGC. Fungsi AGC adalah menghubungkan pengukuran line flow, frekuensi dan data pembangkitan dari infrastruktur SCADA. Tujuan AGC dalam sistem tenaga adalah untuk mengoreksi pembangkitan dengan perubahan beban untuk memelihara frekuensi grid pada 60 Hz. Saat ini, konsep *real time* WAC menggunakan data PMU masih belum memiliki penerapan yang terstandarisasi untuk dijalankan dalam wilayah luas. Potensi penerapan WAC adalah kendali tegangan sekunder menggunakan data PMU, kendali *Static VAR Compensator* (SVC) menggunakan PMU, redaman osilasi inter-area.

2.3 *Phasor Measurement Unit*

Phasor Measurement Unit (PMU) adalah sebuah perangkat yang menghasilkan fasor, frekuensi, dan laju perubahan frekuensi tersinkronisasi dari sinyal tegangan dan/atau arus dan sebuah sinyal pensinkronisasi waktu [3]. PMU sering disebut sebagai *synchrophasor* karena PMU modern mensikronisasikan berbagai pengukuran fasor dari titik-titik yang berbeda pada grid kepadaa sebuah sumber waktu umum (umumnya menggunakan IRIG-B, sebuah protokol sinkronisasi waktu dengan GPS). *Synchrophasor* terdiri dari pengukuran, sinkronisasi, dan fungsi logging. PMU melakukan pengukuran terhadap karakteristik kelistrikan pada suatu grid, kemudian mengkomunikasikan hasil pengukuran kembali kepada PDCdan sistem T-SCADA [5].

2.3.1 Pengukuran *Synchrophasor*

Pengukuran *synchrophasor* harus tersinkronisasi terhadap waktu UTC dengan akurasi yang disebutkan pada [8]. *Error* fasa sebesar 0.01 radian (0.57 derajat) dalam pengukuran *synchrophasor* akan menyebabkan terjadinya 1% *total vector error* (TVE) yang merupakan nilai *error steady-state* maksimum. *Error* fasa sebesar 0.01 radian menyebabkan *error* waktu ±26 µs untuk sistem 60 Hz dan ±31 µs untuk sistem 50 Hz. Sistem harus memiliki kemampuan untuk menerima referensi waktu dari sumber yang memiliki tingkat kehandalan yang tinggi, seperti *Gloal Positioning System* (GPS), yang dapat menyediakan akurasi waktu untuk menjaga TVE tetap berada di bawah 1% dan menyampaikan informasi indikasi hilangnya sinkronisasi hasil pengukuran. *Flag* indikasi hilangnya sinkronisasi berada dalam field STAT bit 13 dari data output. *Flag* bernilai 1 apabila hilangnya sinkronisasi dapat menyebabkan TVE >1% atau ketika hilangnya sinkronisasi terjadi selama lebih dari 1 menit. *Flag* indikator hilangnya sinkronisasi dapat kembali menjadi 0 apabila akuisisi data telah disikronisasi ulang dalam tingkat akurasi yang dibutuhkan.

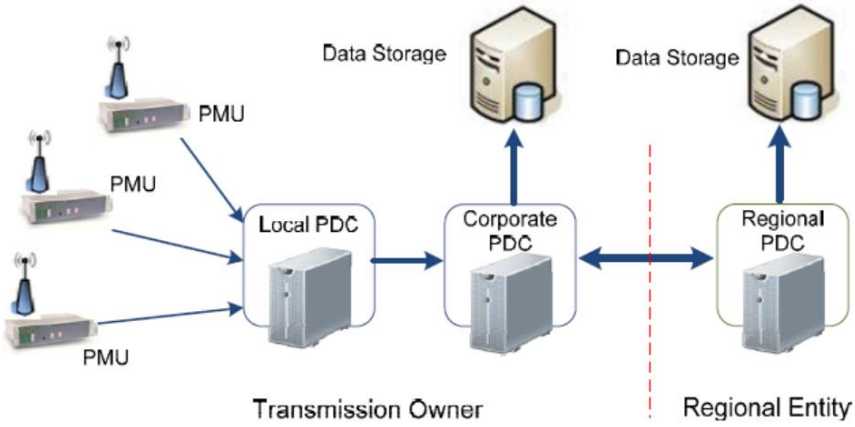
Hasil pengukuran *synchrophasor* ditransmisikan dalam bentuk *frame* data dengan laju F_s yang menyatakan jumlah *frame* per detik atau jumlah detik per *frame* sesuai dengan yang dispesifikasikan pada *field* DATA_RATE dalam *configuration frame*. Sebuah data *frame* adalah himpunan hasil pengukuran yang berasal dari berbagai kanal pengukuran fasor, *analog words*, dan *digital words* dengan sebuah status pengukuran dan sebuah *time tag*. Laju transmisi data yang dibutuhkan untuk sistem PMU dengan frekuensi 50 Hz dan 60 Hz tertera di dalam Tabel II-1.

Tabel II-2 Laju Pelaporan PMU [3]

Frekuensi Sistem	50 Hz			60 Hz					
Laju pelaporan *frame* (*F_s– frames per second*)	10	25	50	10	12	15	20	30	60

2.3.2 Jaringan *Synchrophasor*

Struktur sederhana dari jaringan *synchrophasor* terdiri dari PMU dan PDC. Beberapa PMU ditempatkan pada beberapa gardu induk untuk mengumpulkan data dan mengirimkannya secara *real time* kepada PDC yang terhubung sebagai node agregator data dari beberapa PMU seperti pada Gambar II-3. Aplikasi seperti pengawasan dinamis menggunakan data *real time* dengan resolusi tinggi untuk mendukung fungsi operasi dan perencanaan. Aplikasi menampilkan hasil pengukuran frekuensi, tegangan, arus aliran daya nyata dan reaktif untuk operator sistem.



Gambar II-3 Jaringan *Synchrophasor* [3]

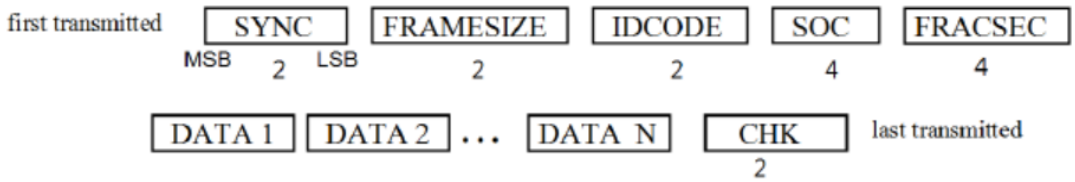
PMU atau PDC dapat mentransmisikan data dalam sebuah atau beberapa aliran data yang terpisah. Setiap aliran dapat berisi konten yang berbeda dan dapat dikirimkan dalam laju yang berbeda. Tujuan untuk setiap aliran *frame* dapat berupa perangkat atau lokasi yang berbeda. Setiap aliran data harus dapat dikontrol, memiliki IDCODE sendiri dan *configuration control* terpisah. Fitur ini berguna untuk mengirimkan data ke perangkat berbeda dengan tujuan yang berbeda, mengijinkan kontrol *latency* dan *class of service* (kelas M dan P) *supply*.

2.3.2 Format Pesan *Synchrophasor*

Terdapat empat jenis pesan (*frame*) yang didefinisikan: *data, configuration, header*, dan *command*.

- *Data frame* merupakan pesan *machine readable* hasil pengukuran yang dikirimkan oleh PMU ke PDC.
- *Configuration frame* adalah pesan *machine readable* yang mendeskripsikan tipe data, faktor kalibrasi, dan meta-data lainnya untuk data yang dikirim PMU untuk melakukan *decode* data.
- *Header frame* adalah informasi deskriptif *human readable* yang dikirim oleh PMU.
- *Command frame* adalah kode *machine-readable* yang dikirim ke PMU untuk melakukan kontrol atau konfigurasi terhadap operasi perangkat pengukuran *synchrophasor*.

Informasi dapat disimpan dalam berbagai bentuk dalam PMU, tetapi ketika ditransmisikan format data harus dalam bentuk *frame* sesuai standar IEEE C37.118.1 . Command dan pesan lain yang tidak dapat dipahami (fitur yang tidak terimplementasi, IDCODE yang salah, CRC buruk) harus disingkirkan. Dalam operasi normal, PMU hanya mengirimkan data *frame*. Format pesan PMU secara umum dapat dilihat pada Gambar II-4.



Gambar II-4 Format Pesan PMU [3]

2.3.2 Sistem Komunikasi PMU

Pesan fasor harus dipetakan secara keseluruhan ke dalam TCP (seperti yang didefinisikan dalam RFC 793) atau UDP (seperti yang didefinisikan dalam RFC 768). Pesan harus dituliskan atau dibaca menggunakan fungsi *input-output* IP sesuai

standar. Nomor *port default* yang digunakan adalah 4712 untuk TCP dan 4713 untuk UDP, tetapi dalam praktiknya, pengguna harus menyebutkan maksud pengaturan nomor *port* yang diinginkan. IP dibawa menggunakan Ethernet atau media transport lainnya. Dengan sebuah *stacked protocol* seperti IP, setiap *layer* pesan dienkapsulasi dalam *layer* di bawah transport *layer* di mana pesan dikirimkan.

Terdapat tiga jenis metode umum dalam sistem komunikasi PMU, yaitu *client-server* di mana transmisi data diinisiasi oleh *command, client* menginisiasi kontak dan mengontrol aliran data sesuai *command*. Metode yang kedua adalah mode dasar operasi yang bersifat spontan di mana *server* mengirim data dengan UDP dan berdasarkan perintah di mana *server* hanya mengirim data ketika *client* meminta penggunaan *command* Start dan Stop standar. Kedua mode tersebut mendukung *command* untuk mendapat data *configuration* dan *header*. Metode umum yang ketiga adalah TCP, UDP, dan komunikasi *multicast*.

BAB III PEMBAHASAN

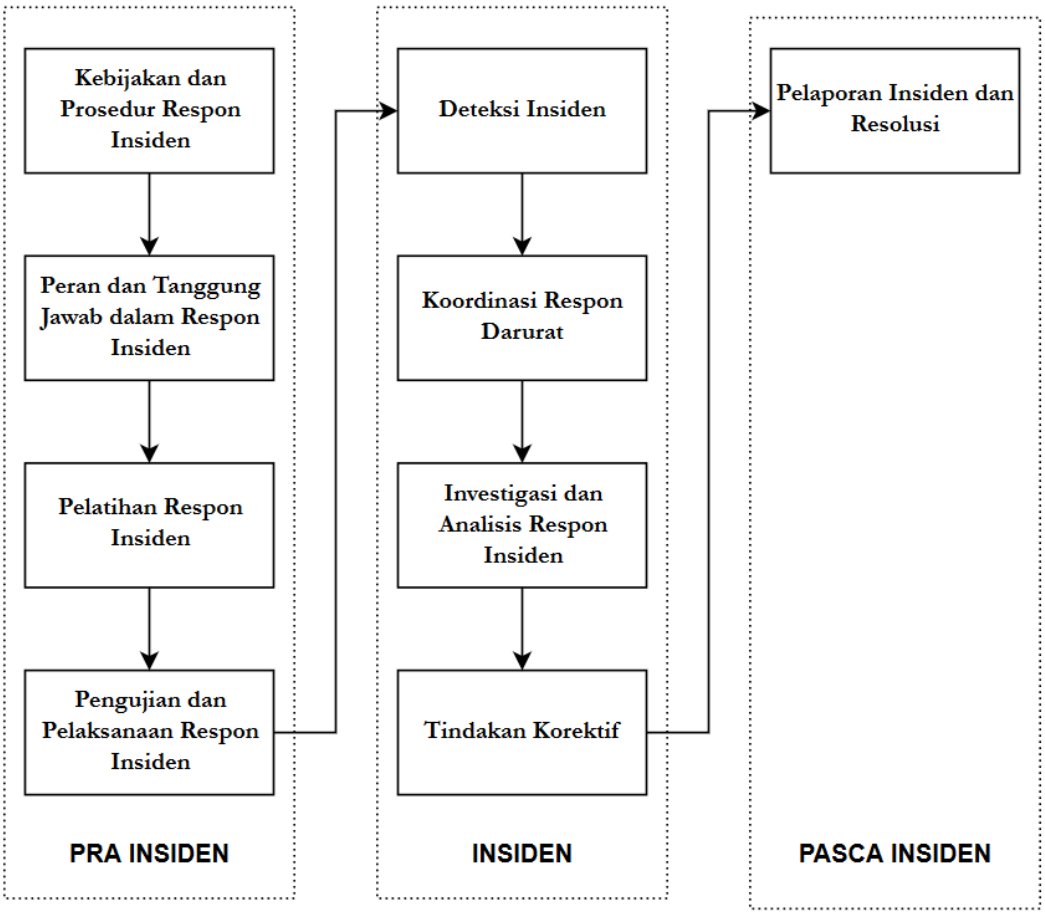
Respon insiden mengacu pada kemampuan untuk melanjutkan operasi sistem informasi *smart grid* dalam kejadian yang mengganggu operasi normal dari sistem informasi samrt grid. Respon insiden memerlukan perencanaan, pengujian, dan pemeliharaan suatu kebijakan dan prosedur tertentu untuk membuat organisasi memulihkan status operasional sistem informasi *smart grid* setelah terjadinya gangguan. Gangguan dapat berasal dari bencana alam, ataupun dibuat oleh manusia (*man made*). Kemampuan sistem informasi *smart grid* untuk menjalankan fungsionalitasnya kembali setelah gangguan secara langsung tergantung pada implementasi kebijakan, prosedur, pelatihan, dan sumber daya sesuai dengan proses perencanaan organisasi. Persyaratan keamanan yang direkomendasikan dalam respon insiden menyediakan kebijakan dan prosedur untuk pengawasan, penanganan, pelaporan, pengujian, pelatihan, dan pemulihan sistem informasi *smart grid* untuk suatu organisasi. Pada Tabel III-1 ditunjukkan beberapa kerentanan respon insiden dalam berbagai bidang di *smart grid*. Kerentanan ini digunakan sebagai salah satu pertimbangan dalam menyusun model respon insiden.

Tabel III-1 Pemetaan Kerentanan Respon insiden

Kelas	Bidang	Kerentanan
Manusia, Kebijakan dan Prosedur	Pelatihan	Kekurangan personel terlatih
		Program kesadaran dan pelatihan keamanan yang tidak memadai
	Kebijakan dan Prosedur	Kebijakan keamanan tidak memadai
		Proses manajemen patch yang tidak memadai
	Manajemen Risiko	Proses respon terhadap insiden yang tidak memadai
Kerentanan Platform	Desain	Penggunaan arsitektur dan desain keamanan yang tidak layak
		Kekurangan peninjauan terhadap desain keamanan oleh pihak eksternal atau rekan

	Implementasi	Perlindungan *malware* yang tidak memadai
	Operasional	Kekurangan patch keamanan terbaru dari vendor perangkat lunak
		Manajemen log yang tidak mencukupi
	Peralatan keamanan yang dkonfigurasi berdasarkan kebijakan	Pelacakan anomali yang tidak memadai

Model respon insiden yang diajukan dalam makalah ini disesuaikan dengan persyaratan keamanan informasi dalam *smart grid* [1] dan disertai dengan rekomendasi implementasinya terhadap PMU. Model yang diajukan untuk menghadapi insiden ditunjukkan pada Gambar III-1. Model proses ini terdiri atas tiga tahapan utama yaitu tahap pra insiden, tahap insiden, dan tahap pasca insiden.



Gambar III-1 Model Respon insiden yang Diajukan

3.1 Tahap Pra-insiden

Tahap pertama dari model proses respon insiden yang diusulkan adalah tahap pra-insiden. Tahap ini terdiri atas empat langkah, yaitu penyusunan kebijakan dan prosedur respon insiden, pendefinisian dan pembagian peran dan tanggung jawab dalam respon insiden, pelaksanaan pelatihan respon insiden, dan pengujian respon insiden.

3.1.1 Penyusunan Kebijakan dan Prosedur Respon insiden

Langkah pertama pada tahap pra-insiden adalah penyusunan kebijakan dan prosedur respon insiden. Pada langkah ini organisasi yang menjalankan sistem *smart grid*, khusunya pada bagian WAMS yang melingkupi sistem kerja PMU, melakukan

pengembangan, peninjauan, dan pembaharuan terhadap dokumen kebijakan respon insiden yang di dalamnya termasuk tujuan dan lingkup program keamanan respon insiden terdahap staf dan pihak ketiga. Langkah ini diperlukan ketika terjadi insiden baru yang belum memiliki kebijakan dan prosedur insiden renspon, pembaharuan patch terbaru dari *vendor* perangkat lunak, pemasangan perangkat atau layanan baru dalam sistem komunikasi yang melibatkan PMU.

Hal yang perlu diperhatikan dalam pelaksanaan langkah ini adalah berbagai jenis insiden dari intrusi sistem perlu diidentifikasi dan diklasifikasikan sesuai dengan efek dan kemungkinannya sehingga respon yang tepat dapat diformulasikan untuk setiap insiden yang potensial. Organisasi menentukan dampak terhadap setiap sistem *smart grid* dan kosekuensinya terkait dengan hilangnya satu atau beberapa sistem informasi *smart grid*. Selain itu, kebijakan dan prosedur yang dibuat wajib mematuhi hukum dan peraturan yang berlaku.

Tabel III-2 Serangan siber dan dampak terhadap PMU

Jenis Serangan	**Vektor Serangan**	**Target Serangan**	**Dampak**
Serangan Denial of Service (DoS)	Via jaringan WAMS, akses RTU	*Bandwidth* sistem komunikasi PMU, layanan pengukuran *real time* fasor oleh PMU	Kegagalan pengaksesan sistem WAMPAC, proses pengukuran PMU tertunda, prediksi yang tidak akurat mengenai status dari sistem transmisi, menunda mitigasi permasalahan dalam sistem tenag
Serangan *Man-in-the-middle*	Via sesi protokol komunikasi antara PMU dan PDC	Hasil pengukuran PMU, data sensitif (*data frame, configuration frame, command frame* IEEE C.37.118)	Modifikasi dan pemalsuan pada data yang ditransmisikan, pembacaan data keadaan tidak akurat dan tidak sesuai dengan keadaan *power grid* yang sebenarnya, mengganggu kehandalan operasional dan keasadaran stabilitas sistem.
Analisis Paket	Via *network*	Informasi *login* dan	Kebocoran kerahasiaan data sensitif

	analyzer (seperti wireshark)	paket data yang ditransmisikan antara PMU dengan perangkat lainnya	
GPS Sppofing	Via GPS receiver PMU	Akurasi *time stamp*	Kesalahan *time stamp* pada data *frame* yang dikirimkan oleh PMU ke perangkat lainnya, kesalahan dalam menganalisis deteksi fault pada line transmisi sistem tenaga dan melakukan pengawasan stabilitas tegangan.
Malicious Code Inection	Via query user input	*Database* sistem informasi	Ekseskusi PMU berubah akibat injeksi *command*.

Sistem *backup* merupakan sitem yang penting diperhatikan dalam menyusun kebijakan dan prosedur respon insden untuk menjaga ketersediaan data dan sistem informasi. Organisasi harus selektif dalam memilih informasi yang harus di-*backup*, persyaratan yang paling utama adalah informasi yang yang berfungsi sebagai bagian dari keberlajutan pengujian operasi. *Backup* yang harus dilakukan adalah informasi *smart grid* pada tingkat sistem (termasuk indormasi keadaan suatu *power grid*), dokumen sistem informasi termasuk dokumentasi terkait keamanan pada organisasi, serta melindungi kerahasiaan dan integritas informasi *backup* pada lokasi penyimpanan. Setelah sistem *backup* terbangun, diperlukan pengujian untuk memverifikasi kehandalan media dan integritas informasi. Organisasi menyimpan salinan *backup* sistem operasi dan perangkat lunak sistem informasi *smart grid* yang penting lainnya dalam fasilitas terpisah, dan tidak dalam lokasi yang sama dengan perangkat lunak operasional. Selain itu, diperlukan keamanan at rest dengan melakukan enkripsi database menggunakan AES-256.

Selain itu, perlu dilakukan perluasan hubungan dengan personel respon darurat lokal dari berbagai cabang untuk meliputi pembagian informasi dan respon terkoordinasi terhadap insiden keamanan siber. Perluasan hubungan salah satunya meliputi pencatatan kontak pihak yang terkait dengan respon insiden sehingga mempermudah

proses koordinasi. Selain itu, dalam langkah ini juga harus disiapkan dokumen-dokumen lengkap seperti topologi jaringan PMU, daftar kontak darurat, penjelasan kerja sistem *backup,* sebagai sarana pendukung prosedur respon insiden.

3.1.2 Pembagian Peran dan Tanggung Jawab dalam Respon insiden

Pada langkah ini, organisasi merancang peran dan tanggung jawab yang spesifik untuk menghadapi insiden dan memulihkan operasi sistem. Setelah itu dilakukan identifikasi personel yang bertanggung jawab terhadap peran-peran yang telah direncanakan. Tim respon insiden yang terbentuk berperan penting dalam mengidentifikasi interupsi dan proses perencanaan. Pembagian peran dan tanggung jawab respon insiden dilakukan dengan menggabungkan jenis peran respon insiden dalam [9] dan [10] dengan menyesuaikan terhadap kebutuhan dalam sistem keamanan PMU.

- *Incident Response Officer*

  Peran ini memiliki akuntabilitas yang tinggi terhadap tindakan tim dan fungsi respon insiden. Peran ini sebaiknya merupakan pegawai yang memiliki tingkatan CISO dan memiliki akses langsung terhadap CEO dan tingkat eksekutif lainnya.

- *Incident Response Manager*

  Peran ini merupakan pemimpin dari tim respon insiden dan mengkoordinasikan aktivitas terkait isiden respon. Peran ini turut bertugas dalam mengevaluasi keamanan, memilih tim respon insiden, dan mengembangkan kebijakan. Peran ini merupakan pihak yang menerima peringatan awal terjadinya insiden dan bertanggung jawab untuk mengaktifkan tim respon insiden dan mengatur proses respon insiden, dari deteksi, penilaian, remediasi dan resolusi. *Incident response manager* wajib melaporkan segala hal terkait insiden kepada *incident response office*r. Peran ini bertujuan untuk menentukan keputusan penting berdasarkan masukan dari incident response *assessment team*.

- *Incident Response Assessment Team*

  Grup ini terdiri dari individu dengan keahlian di bidang yang berbeda. Hal ini bertujuan untuk mengklasifikasikan dan mengambil keputusan dari berbagai disiplin ilmu ketika insiden teridentifikasi. Tim ini pada umumnya mengandung individu-individu dari bidang keahlian sebagai berikut.

  - *Information security*, bertugas dalam melakukan penilaian terhadap kerusakan akibat insiden, mengisolasi insiden, melakukan forensik, dan pemulihan.
  - *IT/MIS*, bertugas dalam meminimalisasi dampak insiden terhadap data organisasi, dan membantu tugas *information security* ketika dibutuhkan.
  - *IT Auditor*, betugas dalam mengobservasi, memahami penyebab insiden, memastikan kepatuhan terhadap prosedur, da berkerjasama dengan *IT/security* untuk menghindari masalah di masa depan.
  - *Security*, bertanggung jawab dalam penilaian kerusakan fasilitas fisik, investigasi bukti fisik, dan menjaga barang bukti selama investigasi forensik berlangsung untuk memelihara randai bukti.
  - *Attorney*, bertanggung jawab dalam memastikan penggunaan bukti yang dikumpulkan selama investigasi yang mana pihak organisasi memilih untuk mengajukan tindakan hukum.
  - *Human Resource*, bertanggung jawab dalam menyediakan saran dalam menangani insiden yang melibatkan pegawai.
  - *Public Relation*, bertanggung jawab dalam berkomunikasi dengan incident response manager untuk memastikan pemahaman yang tepat terhadap madalah dan status organisasi, dan berkomunikas dengan pemilik saham mengenai situasi yang terjadi.
  - *Financial Auditor*, bertanggung jawab dalam menganalisis kemampuan finansial perusahaan dalam menyediakan falisitas terhadap respon insiden serta menganalisis dampak insiden terhadap keuangan organisasi dan

Ketika suatu insiden terjadi, incident response manager mengumpulkan segala rincian terkait insiden, lalu memulai pelacakan dan mendokumentasikan kejadian insiden, dilanjutkan dengan aktivasi incident *response assessment team*. Tim ini wajib melaporkan hasil penilainnya kepada *incident response manager*.

- *Remote Incident Response Coordinator*

  Peran ini dilaksanakan oleh pihak yang memiliki kualifikasi dan kemampuan untuk ditempatkan di wilayah geografi lainnya sebagai pemimpin respon insiden di wilayah tersebut. Peran ini bertugas untuk mengelola respon insiden secara lokal untuk meminimalisasi penyebaran dampak insiden. Peran ini sangat dibutuhkan bagi organisasi yang memiliki bebrapa kantor cabang. Peran ini bertanggung jawab kepada *incident response manager*.

- *Incident Response Custodians*

  Peran ini merupakan individu yang memiliki keahlian teknis dan pendukung aplikasi yang akan dipanggil untuk membantu remediasi dan resolusi terhadap suatu insiden. Pihak ini bertanggung jawab untuk melapor kepada *incident response manager* atau *remote incident response coordinator*, tergantung pada lokasi pihak ini bertugas.

3.1.3 Pelatihan Respon insiden

Pelatihan respon insiden bertujuan untuk melatih personel dalam tim respon insiden sesuai dengan peran dan tanggung jawabnya. Pelatihan wajib dilakukan ketika terdapat suatu kebijakan dan prosedur respon insiden baru. Pelatihan sebaiknya memiliki fasilitas yang terotomatisasi sehingga lingkungan pelatihan menjadi lebih realistis. Setelah dilakukan pelatihan respon insiden, diperlukan evaluasi efektivitas pelatihan terhadap kemampuan personel dalam tim respon insiden maupun pegawai organisasi dalam merespon dan mengatasi insiden. Selain itu, pelatihan juga sebaiknya dilakukan secara berkala untuk menjaga kemampuan pegawai dalam menangani suatu insiden.

3.1.3 Pengujian dan Pelaksanaan Respon insiden

Langkah pengujian dan pelaksanaan respon insiden merupakan langkah akhir dalam persiapan menghadapi insiden yang sesungguhnya. Pengujian dilakukan dengan manjalankan semua kemungkinan insiden yang telah teridentifikasi dan mengimplementasikan langkah penanganan insiden sesuai dengan prosedur terbaru. Pengujian ini bertujuan untuk menguji kemampuan respon insiden dan mengukur efektivitasnya. Hasil pengujian wajib didokumentasikan untuk dianalisis lebih lanjut. Apabila efektivitas prosedur penanganan insiden dinilai masih belum mencukupi, maka tidak diperlukan revisi pembaharuan terhadap kebijakan dan prosedur yang telan disusun dan dilaksanakan kembali pelatihan respon insiden.

3.2 Tahap Penanganan Insiden

Tahap ini dilaksanakan ketika terjadi insiden yang disebabkan oleh pihak tidak berwenang yang bertujuan untuk menghabiskan sumber daya dalam sistem, memperoleh data sensitif, dan mengacaukan sistem yang sedang berlangsung. Pada keadaan seperti ini, tim penanganan insiden wajib mengimplementasikan kemampuannya dalam menangani insiden yang meliputi persiapan, deteksi dan analisis, penahanan, mitigasi, dan pemulihan.

3.2.1 Deteksi Insiden

Deteksi insiden pada PMU salah satunya dapat diindikasikan melalui informasi anomali atau *set flag frame* IEEE C37.118 sebagaimanan yang ditunjukkan dalam Tabel III-3.

Tabel III-3 *Bit mapped flags* pada *field* STAT dalam *frame* IEEE C37.118.

Nomor Bit	Nilai Bit	Jenis Insiden
Bit 15-14 (*Data error*)	01	PMU *error*. Tidak terdapat informasi tentang data
	11	PMU *error*.
Bit 13 (*PMU Sync*)	1	Hilangnya sinkronisasi dengan sumber waktu UTC

Bit 09 (*Data modified*)	1	Data termodifikasi oleh post-processing
Bit 08-06 (*PMU Time Quality*)	111	Perkiraan *error* waktu maksimum > 10 ms atau *error* waktu tidak diketahui
	110	Perkiraan *error* waktu maksimum < 10 ms
	101	Perkiraan *error* waktu maksimum < 1 ms
	100	Perkiraan *error* waktu maksimum < 100 µs
	011	Perkiraan *error* waktu maksimum < 10 µs
	010	Perkiraan *error* waktu maksimum < 1 µs
	001	Perkiraan *error* waktu maksimum < 100 ns
	000	Tidak digunakan
Bit 05-04 (*Unlocked time*)	00	*Locked* atau *unlocked* kurang dari 10 s
	01	*Unlocked* 10 s atau lebih lama tetapi kurang dari 100s
	10	*Unlocked* 100s atau lebih lama tetapi kurang dari 1000 s
	11	*Unlocked* 1000 s atau lebih

Selain melalui informasi bit dalam *frame* data yang ditransmisikan PMU, deteksi juga dapat dilakukan melalui kode peringatan yang ditunjukkan pada parameter keamanan seperti IDS yang terpasang pada *gateway* keamanan PMU.

3.2.2 Koordinasi Respon Darurat

Setelah suatu insiden terdeteksi, maka harus segera dilakukan koordinasi respon darurat dengan menghubungi pihak-pihak yang yang bertanggung jawab dalam penanganan insiden di suatu daerah yang bersangkutan. Koordinasi dilakukan dengan menggunakan dokumen kontak pihak-pihak penting yang meliputi pegawai di organisasi tersebut atau pihak ketiga seperti *provider* layanan internet, *software developer*, atau pihak lain yang terkait terhadap peristiwa insiden di suatu wilayah. Koordinasi kontak darurat harus berisi beberapa pilihan dalam menguhubungi pihak terkait, sehingga tidak hanya tergantung pada suatu media komunikasi saja. Koordinasi respon darurat dapat dilakukan melalui internet (email, atau messenger Facebook, Telegram, WhatsApp, Line, Hangouts), kabel telepon, atau sinyal radio.

3.2.3 Investigasi dan Analisis Respon insiden

Setelah laporan insiden diterima, dilakukan investigasi dan analisis terhadap insiden yang terjadi beserta evaluasi efektivitas penanganan insiden yang telah dilakukan. Langkah ini bertujuan mehamami karakteristik insiden untuk keperluan pengembangan kebijakan dan prosedur respon insiden, program analisis dalam program perencanaan yang akan datang sehingga memberikan cara yang efektif dalam menangani suatu insiden. Segala aktivitas investigasi dan analisis respon insiden wajib didokomentasikan. Investigasi dilakukan dengan mengamankan log dan media (perangkat keras dan aplikasi) yang menjadi sasaran dalam suatu insiden.

3.2.4 Tindakan Korektif

Langkah ini bertujuan untuk meninjau hasil investigasi dan menentukan tindakan korektif yang dibutuhkan. Lalu memasukkan proses dan mekanisme tindakan korektif dalam perencanaan untuk memastikan bahwa tindakan korektif telah diidentifikasi sebagai hasil dari insiden sistem informasi *smart grid* dan keamanan siber, sepenuhnya diimplementasikan. Dalam menentukan tindakan korektif, sebaiknya dilakukan petukaran informasi insiden antar organisasi untuk memahami pengalaman dari pihak lain.

3.3 Tahap Pasca Insiden

Tahap ini dilaksanakan ketika kejadian insiden telah berakhir/tidak aktif. Terdapat beberapa langkah yang perlu dilakukan dalam tahap pasca insiden ini, di antaranya adalah pengawasan insiden, pelaporan insiden, investigasi dan analisis respon insiden, tindakan korektif, sistem backup informasi *smart grid*, dan koordinasi respon darurat.

3.3.1 Pelaporan Insiden dan Resolusi

Pelaporan insiden wajib meliputi definisi insiden terjadi, dampaknya terhadap sistem informasi, dilengkapi dengan *time stamp* untuk setiap rinci kejadian insiden.

Pelaporan insiden kepada *incident response assessment team* dilakukan melalui *trusted path* yang menggunakan sistem autentikasi. Selain pelaporan insiden yang telah terjadi, juga disertakan resolusi untuk meningkatkan efisiensi dan efektivitas respon insiden untuk dijadikan bahan pertimbangan dalam perumusan kebijakan dan prosedur insiden respon yang baru.

BAB IV KESIMPULAN

Dalam makalah ini, diajukan suatu pemodelan respon insiden yang bertujuan untuk menangani insiden yang terjadi pada PMU secara efektif. Model ini melihat efektivitas suatu respon insiden tidak hanya tergantung pada proses penanganan saat insiden terjadi, melainkan juga mempertimbangkan pentingnya rangkaian kegiatan pada saat sebelum terjadinya insiden dan setelah terjadinya insiden sebagai komponen penting yang mempengaruhi efektivitas respon insiden.

Model respon insiden terdiri atas tiga tahap, yaitu tahap pra insiden, tahap insiden, dan tahap pasca insiden, di mana setiap tahap terdiri atas beberapa langkah. Tahap pra-insiden yang meliputi kegiatan penyusunan kebijakan dan prosedur, pembagian peran dan tanggung jawab, pelatihan, dan pengujian respon insiden sebagai kegiatan yang dapat meningkatkan kesiapan dan kematangan sistem dalam menghadapi insiden. Tahap terjadinya insiden meliputi deteksi insiden, koordinasi respon darurat, investigasi dan analisis respon insiden, dan tindakan korektif yang bertujuan untuk menangani insiden secara tepat dan efektif. Pasca terjadinya insiden, dilakukan pelaporan insiden dan resolusi. Model insiden respon ini bersifat terbuka dan memanfaatkan perubahan dan hal-hal baru dari suatu kejadian insiden sebagai bahan dalam merumuskan prosedur dan kebijakan yang terbaru dan membuat komunikasi antar pihak yang terlibat dalam respon insiden menjadi lebih terkoordinasi

BAB V DAFTAR REFERENSI

[1] Smart Grid Cybersecurity Commitee, "Guidelines for Smart GRid Cybersecurity: Smart Grid Cybersecurity Strategy, Architecture, and High-Level Requirements," NIST, Gaithersburg, NIST 7628 Revision 1, 2014.

[2] Hugh Melvin, "The Role of ICT in Evolving SmartGrids," , Galway, 2012.

[3] IEEE Power & Energy Society, "IEEE Standard for Synchrophasor Data Transfer for Power System," IEEE Standard Association, New York, IEEE Std C37.118.2, 2011.

[4] J. Ivanovski, V. Maden, "PMU Traffic Scenarios and Network Conditions in IP-Based Wide Area," Royal INstitute of Technology, Stockholm, Master Thesis Report 2009.

[5] Knapp E., Samani R., *Applied Cyber Security and the Smart Grid: Implementing Security Controls into the Modern Power Infrastructure*, Joel Langill, Ed. Waltham, USA: Sngress, 2013.

[6] M. Qiu, H. Su, M. Chen, Z. Ming, L.T.Yang, "Balance of Security Strength and Energy for a PMU Monitoring System in Smart Grid," *IEEE Communication Magazine*, pp. 142-149, May 2012.

[7] V. Terzija, D. Cai, S. Skok, A. Phadke, "Wide-Area Monitoring, Protection, and Control of Future Electric Power Network," *Proceedings of the IEEE*, vol. 99, no. 1, pp. 80-93, Agustus 2010.

[8] IEEE Power & Energy Society, "IEEE Standard for Synchrophasor Measurements for Power System," IEEE, New York, IEEE Standard IEEE Std C37.118.1, 2011.

[9] Jesse Valentin. (2013, Februari) Infosec Security - IT Security. [Online]. http://resources.infosecinstitute.com/building-an-incident-response-team-and-ir-process/

[10] Michelle Borodkin, "Computer Incident REsponse Team," *Information Security*

Reading Room, 2001.