JPPI Vol 6 No 1 (2016) 59 – 78

Jurnal Penelitian Pos dan Informatika
578/AKRED/P2MI-LIPI/07/2014

e-ISSN: 2476-9266
p-ISSN: 2088-9402

DOI: 10.17933/jppi.2016.060104

PENINGKATAN KEAMANAN *SUPERVISORY CONTROL AND DATA ACQUISITION* (SCADA) PADA *SMART GRID* SEBAGAI INFRASTRUKTUR KRITIS

IMPROVED SECURITY SUPERVISORY CONTROL AND DATA ACQUISITION (SCADA) THE SMART GRID AS CRITICAL INFRASTRUCTURE

Ahmad Budi Setiawan

Puslitbang APTIKA dan IKP – Kementerian Komunikasi dan Informatika
Jalan Medan Merdeka Barat Jakarta 10110 - Indonesia
ahma003@kominfo.go.id

Naskah Diterima: 15 April 2016; Direvisi: 23 Agustus 2016; Disetujui: 25 September 2016

Abstrak

SCADA (Pengawas Control dan Data Acquisition) sistem sebagai unit kontrol *smart grid* telah digunakan di hampir berbagai industri di seluruh dunia dalam hal sistem otomatisasi. *smart grid* menggabungkan infrastruktur energi dan telekomunikasi dan jaringan Internet. Sistem ini memberikan kemudahan operasional dan efisiensi dalam industri. Namun, sistem memiliki banyak kerentanan dalam aspek keamanan informasi yang dapat berdampak besar bagi industri dan bahkan ekonomi. Penelitian ini mencoba untuk merancang dalam membangun keamanan jaringan maya pintar, itu termasuk strategi yang harus dilakukan dan informasi sistem keamanan arsitektur yang akan dibangun. Penelitian dilakukan kualitatif wawancara mendalam, diskusi kelompok terfokus dan observasi langsung. Hasil dari penelitian ini adalah rekomendasi strategi desain pada pengembangan keamanan *smart grid cyber*. Rekomendasi penelitian ini juga dimaksudkan sebagai kerangka saran-membuat untuk keamanan *smart grid cyber* sebagai acuan pelaksanaan *smart grid* di Indonesia.

Kata kunci: Smart Grid, SCADA, Cyber Security, Risk Management

Abstract

SCADA (Supervisory Control and Data Acquisition) systems as the control unit of the smart grid has been used in almost various industries around the world in terms of automation systems. Smart grid technology combines the energy infrastructure and telecommunications and Internet networks. The system provides the operational ease and efficiency in the industry. However, the system has a lot of vulnerabilities in information security aspects that can have a major impact for the industry and even the economy. This study tried to design in building a smart grid cyber security, it includes the strategies that must be done and the information security system architecture to be built. The study was conducted qualitative in-depth interviews, focus group discussions and direct observation. Results of this research are the design strategy recommendations on the development of smart grid cyber security. Recommendation of this study also intended as a suggestion-making framework for smart grid cyber security as a reference implementation of the smart grid in Indonesia.

***Keywords**: Smart Grid, SCADA, Cyber Security, Risk Management*

PENDAHULUAN

Sistem SCADA digunakan hampir berbagai industri di dunia, namun para stakeholder kebanyakan tidak menyadari pentingnya hal tersebut terkait kerentanan dari sistem SCADA. Sistem SCADA yang digunakan untuk mengontrol aset tersebar menggunakan akuisisi data terpusat dan kontrol pengawasan. Sistem kontrol sangat penting untuk pengoperasian infrastruktur kritis bagi negara yang mana sistem yang sangat saling berhubungan dan saling bergantung.

Smart grid merupakan sebuah konsep sistem control yang kompleks untuk mengelola dan mentransmisikan energi kepada konsumen. Sistem kontrol merupakan isu yang sangat penting untuk melakukan efisiensi dalam penanganan operasional infrastruktur kritis seperti Sistem *Smart grid* terkait dalam ketersediaan pasokan listrik. Sistem melakukan interkoneksi antara beberapa sistem yang mendukung *smart grid*, melakukan upgrade jaringan listrik yang masih tradisional dengan sistem kontrol dan jaringan yang dapat meningkatkan efisiensi dan memberikan metode baru untuk mengelola sistem.

Infrastruktur *Smart grid* merupakan salah satu infrastruktur kritis karena berperan sebagai pengatur energi penting bagi masyarakat dan ekonomi. Perusakan terhadap infrastruktur kritis akan mendatangkan dampak terhadap perekonomian Dorantes (2006 pp. 13-22). Teknologi *smart grid* menggabungkan antara infrastruktur energi dan telekomunikasi serta jaringan internet. Dengan demikian, *smart grid* harus beroperasi dengan aman dan menghormati privasi pengguna akhir. Dalam kasus pembangkit energi ketenagalistrikan, perlindungan *smart grid* adalah kunci untuk ketersediaan energi. Sehingga diperlukan suatu panduan dokumen yang menguraikan isu-isu keamanan dunia maya (*cyber space*) berkaitan dengan infrastruktur informasi *smart grid*.

Smart grid merupakan evolusi dari jaringan listrik untuk merespon tantangan saat ini.Sebuah *smart grid* adalah transmisi energi dan jaringan distribusi yang ditingkatkan melalui kontrol secara digital, pemantauan, dan kemampuan telekomunikasi. *Smart grid* menyediakan sistem real-time, aliran dua arah komunikasi dan penyedia informasi untuk semua pemangku kepentingan dalam semua rantai listrik, Mulai dari pemegang saham sampai ke pengguna akhir komersial, industri, dan perumahan.

Keamanan terhadap infrastruktur kritis merupakan prasyarat mutlak yang harus diimplementasikan agar dapat menjamin efektifitas keandalan, ketersediaan dan integritas jaringan informasi, baik secara nasional maupun global M. Hendrson (2007). Kebutuhan untuk integrasi teknologi komunikasi dan informatika sangat diperlukan untuk menggabungkan beberapa operator energi dan kebutuhan distribusi energi. Namun disisi lain penggabungan antara listrik dengan telekomunikasi jaringan akan memunculkan permasalahan baru sehingga membutuhkan penilaian risiko secara keseluruhan pada keandalan operasi jaringan dan sistem manajemen. Interkoneksi sistem yang kompleks dari generator ke konsumen melalui standar protokol terbuka akan membawa tantangan serius dalam hal penanganan keamanan sistem secara keseluruhan.

Perlindungan *smart grid* adalah kunci untuk ketersediaan energi. Sehinggadiperlukan suatu

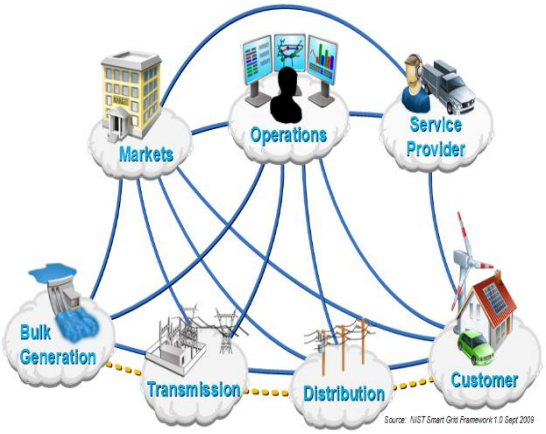
panduan dokumen yang menguraikan isu-isu keamanan dunia maya (*cyberspace*) berkaitan dengan infrastruktur informasi *smart grid.*Secara garis besar penelitian ini mencoba melakukan perancangan bagaimana membagun smartgrid cyber security, hal ini termasuk bagaimana strategi yang harus dilakukan, bagaimanaarsitektur yang harus dibangun dan bagaimana tahapan migrasi yang harus dijalankan. Hasil penelitian ini adalah rekomendasi peningkatan keamanan SCADA dalam pengembangan *smart grid* cyber security. Rekomendasi hasil penelitian ini juga bertujuan sebagai rekomendasi pembuatan kerangka kerja (*framework*) untuk *smart grid* cyber securitysebagai bahan acuan penerapan *smart grid* di Indonesia.

SMART GRID Ketenagalistrikan

Smart grid terdiri atas 3 (tiga) unsur penting, yakni teknologi informasi, telekomunikasi dan tenaga listrik. Ketiga unsur tadi bekerja sama untuk memungkinkan adanya komunikasi 2 arah antara utility company seperti sebuah perusahaan listrik dengan konsumen. Dengan *smart grid*, transfer energi listrik yang terjadi tidak hanya dari perusahaan penyedia listrik ke konsumen, namun juga sebaliknya. Jika ternyata konsumen memiliki solar cell yang dapat menghasilkan energi listrik dari cahaya matahari, maka ketika energi listrik dari solar cell itu melebihi dari besar kebutuhan konsumen itu, maka konsumen bisa mengirim energi listrik ke grid yang ada National Institute of Standard and Technology (2010). Konsumen bisa mendapatkan uang dari utility sistem atas hal tersebut.

Perlindungan Infrastruktur Kritis

Perlindungan infrastruktur kritis adalah sebuah konsep yang berhubungan dengan kesiapan dan respon terhadap insiden serius yang melibatkan infrastruktur kritis suatu wilayah atau bangsa. Bahwa ketidakmampuan atau penghancuran sistem tersebut dan aset akan memiliki dampak melemahkan keamanan negara, keamanan ekonomi nasional, kesehatan masyarakat secara nasional dan keselamatan suatu bangsa. Sistem dan jaringan yang membentuk infrastruktur secara nasional biasanya merupakan suatu sistem utuh yang kuat, namun gangguan pada salah satu sistem dapat memiliki konsekuensi yang berbahaya bagi sektor lain Keith Stouffer (2011) dalam National Institute of Standard and Technology (2007)



Gambar 1. Konsep *Smart grid* Ketenagalistrikan

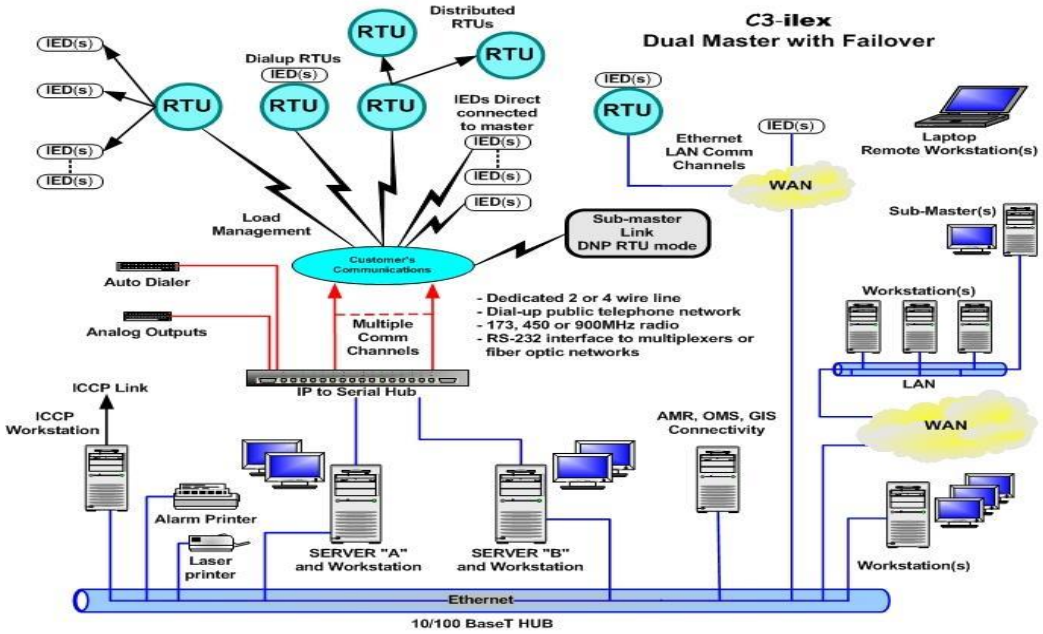
Sistem Kontrol Industri

Sistem kontrol industri (*SMART GRID*) adalah istilah umum yang mencakup beberapa jenis sistem kontrol yang digunakan dalam produksi industri, termasuk sistem SCADA, sistem kontrol terdistribusi(DCS), dan konfigurasi sistem kontrol yang lebih kecil lainnya seperti *Programmable Logic Controller* (PLC) sering ditemukan pada sektor industri dan infrastruktur kritis. *SMART GRID* biasanya digunakan dalam industri seperti listrik, air, minyak, gas dan manufaktur.

Berdasarkan data yang diterima dari stasiun jarak jauh, otomatis atau melalui perintah pengawasan operator yang dikirim ke perangkat kontrol stasiun jarak jauh, yang sering disebut sebagai perangkat lapangan. Perangkat lapangan mengendalikan operasi lokal seperti membuka dan menutup katup dan pemutus aliran listrik, mengumpulkan data dari sistem sensor, dan pemantauan lingkungan setempat untuk kondisi tertentu Federal Energy Regulatory Commission (2013)

SCADA

Supervisory Control and Data Acquisition (SCADA) adalah sistem yang berfungsi untuk memberikan instruksi kendali dan mengawasi kerja suatu proses tertentu. Data Acquisitionadalah sistem yang berfungsi untuk mengambil, mengumpulkan, dan memproses data untuk kemudian disajikan sesuai kebutuhan yang dikehendaki. SCADA dapat diartikan sistem berbasis komputer yang dapat melakukan pengawasan, pengendalian, dan akuisisi data terhadap suatu proses tertentu secara real time M. Winanda (2014) dalam Gary J. Finco (2006).



Gambar 2. Arsitektur Sistem SCADA

Arsitektur SCADA menurut E. H. Gary J. Finco (2006) terdiri dari:

- Plant/field device (perangkat lapangan): suatu proses di lapangan yang diwakili oleh sensor dan aktuator.
- RTU (Remote Terminal Unit): Berupa PLC, berfungsi sebagai pengendali plant/field device, mengirim sinyal kontrol, mengambil data dari plant, mengirim data ke MTU.
- MTU (Master Terminal Unit): Berupa PLC, MTU bertindak sebagai master bagi RTU, MTU berfungsi mengumpulkan data dari satu atau beberapa RTU, melakukan koordinasi dengan memberi perintah ke RTU untuk menjaga agar proses berjalan dengan stabil dan memberikan data ke server/HMI.

- HMI (Human Machine Interface): Menampilkan data pada suatu perangkat yang komunikatif dan animatif, menyediakan antarmuka komunikasi antara mesin dengan manusia (operator).
- Protokol komunikasi: sebuah aturan atau standar yang mengatur atau mengijinkan terjadinya hubungan, komunikasi, dan perpindahan data antara dua atau lebih titik komputer.
- Database Server: mencatat data pengendalian

Adapun keuntungan penggunaan SCADA adalah:

- Mampu mengendalikan proses-proses yang kompleks
- Akses pengukuran kuantitatif dari proses-proses yang penting secara *real time*.
- Mendeteksi dini dan memperbaiki kesalahan secara cepat
- Mempermudah proses evaluasi kinerja untuk peningkatan efisiensi, dan
- Penghematan biaya.

METODE

Penelitian ini dilakukan dengan metode kualitatif. Secara garis besar penelitian menggunakan metode kualitatif dengan cara; mengumpulkan data kualitatif, kajian literatur dan menerapkan best practice atau standar untuk merancang panduan dalam rangka peningkatan keamanan SCADA pada *smart grid* W. Cresswell(2008).

Penelitian kualitatif ini menggunakan penelitian pendekatan studi kasus. Menurut Penelitian kualitatif adalah penelitian yang menghasilkan dan mengolah data yang sifatnya deskriptif, seperti transkripsi wawancara , catatan lapangan, gambar, foto rekaman video dan lain-lain. Dalam penelitian kualitatif perlu menekankan pada pentingnya kedekatan dengan orang-orang dan situasi penelitian, agar peneliti memperoleh pemahaman jelas tentang realitas dan kondisi kehidupan nyata.

Sedangkan studi kasus adalah uraian dan penjelasan komprehensif mengenai aspek seorang individu, suatu kelompok, suatu organisasi (komunitas), suatu program, atau suatu situasi sosial. Peneliti studi kasus berupaya menelaah sebanyak mungkin data mengenai subjek yang diteliti.

Tahap-tahap penelitian

Dalam penelitian terdapat dua tahap penelitian, yaitu :

Tahap Persiapan Penelitian

Pertama peneliti melakukan studi literature untuk memahami substansi dan mendalami lebih jauh permasalahan penelitian. Berdasarkan hal tersebut, dirumuskan pedoman pertanyaan indeepth interview dan pedoman pertanyaan *Focus Group Discussion* (FGD) yang disusun berdasarkan permasalahan yang dihadapi subjek. Pedoman pertanyaan wawancara mendalam (*indeepth interview*) dan FGD ini berisi pertanyaan-pertanyaan mendasar yang nantinya akan berkembang dalam diskusi. Pedoman pertanyaan

Indeepth interview yang telah disusun, ditunjukan kepada para pakar dan praktisi, dalam hal ini adalah pembibing penelitian untuk mendapat masukan mengenai isi pedoman pertanyaan *indeepth interview*. Setelah mendapat masukan dan koreksi dari pembimbing, peneliti membuat perbaikan terhadap pedoman pertanyaan *indeepth interview* dan FGD dan mempersiapkan diri untuk melakukan *in-dept interview* dan diskusi.

Peneliti selanjutnya mencari informan yang sesuai dengan karakteristik subjek penelitian. Untuk itu sebelum wawancara dan FGD dilaksanakan peneliti bertanya kepada informan tentang

kesiapanya untuk wawancara dan berdiskusi. Setelah subjek bersedia untuk diajak wawancara dan berdiskusi, peneliti membuat kesepakatan dengan subjek tersebut mengenai waktu dan tempat untuk melakukan diskusi.

Tahap pelaksanaan penelitiaan

Peneliti membuat kesepakatan dengan informan mengenai waktu dan tempat untuk melakukan wawancara dan diskusi berdasarkan pedoman yang dibuat. Setelah wawancara dan diskusi dilakukan, peneliti memindahakan hasil rekaman berdasarkan diskusi dalam bentuk tertulis. Selanjutnya peneliti melakukan analisis data dan interprestasi data sesuai dengan langkah-langkah yang dijabarkan pada bagian metode analisis data di akhir bab ini.

Teknik Pengumpulan Data

Dalam penelitiaan ini, peneliti menggunakan 3 teknik pengumpulan data, yaitu :

1. *In-depth Interview*

Wawancara mendalam (indeepth interview) dilakukan oleh dua pihak yaitu komunikasi antara peneliti dengan informan.

2. *Observasi*

Disamping diskusi, penelitian ini juga melakukan metode observasi dengan melakukan pengamatan dan pencatatan secara sistimatik terhadap unsur-unsur yang tampak dalam suatu gejala atau gejala-gejala dalam objek penelitian.

Dalam penelitian ini observasi dibutuhkan untuk dapat memehami proses terjadinya diskusi dan hasil diskusi dapat dipahami dalam konteksnya. Observasi yang akan dilakukan adalah observasi terhadap subjek, perilaku subjek selama wawancara, interaksi subjek dengan peneliti dan hal-hal yang dianggap relevan sehingga dapat memberikan data tambahan terhadap hasil wawancara.

HASIL DAN PEMBAHASAN

Infrastruktur listrik secara tradisional dilihat dari segi pembangkit listrik stasiun pusat menyediakan listrik kepada pelanggan atau konsumen.Secara tradisional di fasilitas pelanggan, beban disajikan tanpa banyak administrasi atau kontrol terhadap konsumsi listrik selain berjalan dan metering perangkat listrik atau peralatan. Sebagai teknologi mulai berkembang, pengelolaan dan pengendalian peralatan dan beban berevolusi. Hal ini termasuk peralatan dan beban yang baik diatur untuk beroperasi pada jadwal atau yang memonitor parameter tertentu dan akan mengkomunikasikan informasi tersebut untuk controller (peralatan atau orang) untuk sengaja mempekerjakan beberapa metode atau cara untuk mengelola konsumsi listrik atau pengirimannya.

Sebagai teknologi berkembang lebih lanjut, sumber daya didistribusikan (baik generator dan sistem penyimpanan listrik) yang saling berhubungan dengan sistem kekuasaan.Hari ini, komunikasi dan sistem informasi memungkinkan, sistem tenaga yang lebih cerdas modern. Terpadu, sepenuhnya otomatis pendekatan *smart grid* dapat memungkinkan pilihan produktif untuk kedua operator utilitas dan pelanggan untuk meningkatkan keandalan sistem tenaga, pemanfaatan aset, dan efisiensi, dengan cara yang aman.

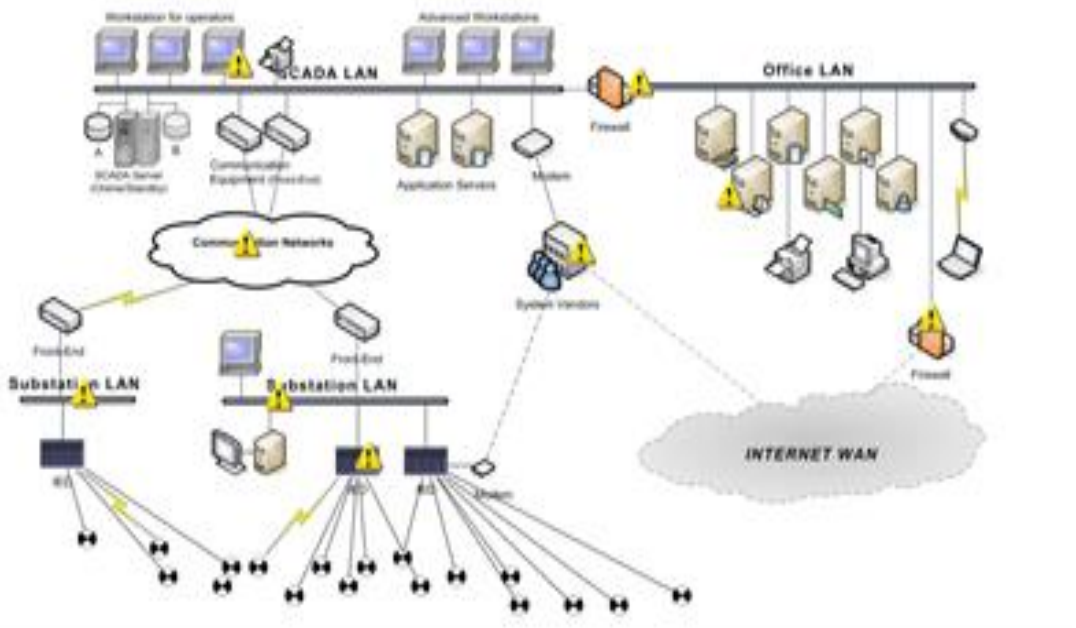
Supervisory Control and Data Acquisition (SCADA) merupakan sistem yang biasanya digunakan untuk pemantauan dan pengendalian operasi yang berlokasi jauh secara geografis. Meskipun sistem SCADA digunakan pada hampir

berbagai industri di dunia, namun para stakeholder kebanyakan tidak menyadari pentingnya hal tersebut terkait kerentanan dari sistem SCADA. Sistem SCADA yang digunakan untuk mengontrol aset tersebar menggunakan akuisisi data terpusat dan kontrol pengawasan. Sistem kontrol sangat penting untuk pengoperasian infrastruktur *smart grid* yang mana sistem yang sangat saling berhubungan dan saling bergantung menurut P. A. Metin Ozturk (2011) dalam Sauver (2004).

Area *Smart grid* dimana ancaman siber sangat berpeluang untuk terjadi:

1. Teknologi Informasi untuk sistem operasi
   - Sistem Grid SCADA
   - Sistem Data Acquisition System (DAS)
   - Outage Management System/ Distribution Management
   - Sistem dari DISCOM
   - Advanced Metering Infrastructure (AMI)
2. Teknologi informasi untuk fungsi bisnis
   - Metering, penagihan dan penyimpanan data
   - Web Portal konsumen
   - Sistem IT untuk internal organisasi
3. Sistem komunikasi untuk koordinasi
   - Komunikasi antara operator dan komunikasi data
   - Node pertukaran / pengolahan data

Gambar berikut ini menunjukkan potensi lokasi serangan siber pada *Smart grid*



Gambar 3. Potensi lokasi serangan siber
Sumber: Gunnar Björkman, ABB Mannheim

Serangan Smart grid

Sementara teknologi ini menawarkan manfaat yang besar, namun juga memperkenalkan risiko jenis baru, terutama menciptakan vektor serangan baru yang dapat dimanfaatkan oleh penyerang sebagai contoh adalah berikut:

- *Smart grid* control sistem
- Gangguan dan pemblokiran lalu lintasInformasi
- *Smart grid* terinfeksi oleh Malware

Hal tersebut dapat terjadi di Pembangkit Listrik, transmisi maupun sistem distribusi. Damapak serangan dari masing-masing jenis serangan tersebut dapat dilihat pada Tabel 1 berikut ini

Tabel 1. Dampak Serangan Keamanan *Smart grid*

No	Jenis Serangan	Kemungkinan Dampak	Lokasi
1	SCADA	Confidentiality, denial of service, integrity	LAN
2	Smart meter	Confidentiality, integrity, availability, non repudiation	LAN/Jaringan Mitra
3	Layer Fisik	Data integrity, denial of service, confidentiality	LAN/Jaringan Mitra/WAN
4	Data injection dan replay attacks	Confidentiality	LAN/Jaringan Mitra/WAN
5	Basis jaringan	Availability, confidentiality	LAN/Jaringan Mitra/WAN

Sumber: Gunnar Björkman, ABB Mannheim
*Smart grid*s Security SICS Security Seminar on April 8, 2014

Ancaman siber juga berkembang dan menjadi sangat canggih. Advanced Persistent Threats (APT) adalah ilustrasi yang baik dari perkembangan ini.Bukan hanya terkait penyerang amatir, tetapi penyerang profesional yang sangat terampil dan terorganisir mampu melancarkan serangan yang kompleks dan terkoordinasi dengan menggunakan alat-alat canggih. Banyak jenis ancaman cyber yang terkenal:

- Hijack
- Malware
- Denial of service (DOS)
- Distributed denial of service (DDOS).

Dampak Serangan siber di *Smart grid*

- Serangan siber menyebabkan gangguan listrik pada infrastruktur *Smart grid* terkait operasional pasokan energi dan akan membuat " Black Out dan chaos" dalam kegiatan ekonomi dan bisnis, kegiatan politik dan kegiatan sosial.
- Mengambil lebih banyak waktu digunakan untuk mengurangi atau menghilangkan situasi"Chaos"

Sistem kontrol *smart grid* memiliki sedikit kemiripan dengan sistem teknologi informasi tradisional, dimana *smart grid* merupakan sistem terisolasi yang sering kali menggunakan protokol kontrol eksklusif menggunakan perangkat keras khusus dan perangkat lunak khusus. Namun saat ini sudah mulai banyak yang memakai perangkat *Internet Protocol* (IP) yang menggantikan solusi *proprietary*, yang meningkatkan kemungkinan terjadinya kerentanan dan insiden keamanan siber menurut Adam Hahn (2013) dalam K. Zedda (2010)

Meskipun beberapa karakteristik yang mirip, *smart grid* juga memiliki karakteristik yang berbeda dari sistem pengolahan informasi tradisional. Beberapa perbedaan *SMART GRID* adalah bahwa *SMART GRID* ketika terjadi eksekusi memiliki pengaruh langsung terhadap dunia fisik. Beberapa karakteristik ini meliputi risiko yang signifikan terhadap kesehatan dan keselamatan jiwa manusia dan kerusakan serius pada lingkungan, serta isu-isu keuangan serius seperti kerugian industry akibat tidak ada pasokan listrik, dampak negatif terhadap perekonomian suatu negara.

Ancaman terhadap sistem kontrol dapat datang dari berbagai sumber, termasuk negara musuh, kelompok teroris, karyawan yang tidak puas, penyusup yang berbahaya, kompleksitas operasional, kecelakaan operasional, bencana alam serta tindakan berbahaya atau tidak disengaja oleh karyawan. Tujuan keamanan *SMART GRID* mengikuti prioritas ketersediaan, integritas dan kerahasiaan. Insiden *SMART GRID* yang mungkin sebagai berikut:

- Diblokir atau tertunda arus informasi melalui jaringan *SMART GRID*, yang bisa mengganggu pengoperasian *SMART GRID*
- Perubahan tidak sah terhadap instruksi, perintah, atau ambang batas alarm, yang dapat merusak, melumpuhkan,atau mematikan peralatan, membuat dampak lingkungan, dan/atau membahayakan kehidupan manusia
- Informasi yang tidak akurat dikirim ke operator sistem, baik untuk menyamarkan perubahan tidak sah, atau menyebabkan operator untuk melakukan tindakan yang tidak sesuai, yang bisa memiliki berbagai efek negatif
- Pengaturan *SMART GRID* perangkat lunak atau konfigurasi diubah, atau perangkat lunak *SMART GRID* terinfeksi dengan *malware*, yang bisa memiliki berbagai efek negatif

Interferensi dengan pengoperasian sistem keselamatan, yang bisa membahayakan kehidupan manusia.

Tujuan keamanan utama dalam implementasi *SMART GRID* harus mencakup sebagai berikut:

- Membatasi akses logis untuk jaringan *SMART GRID* dan aktivitas jaringan. Ini termasuk menggunakan zona demiliterisasi (DMZ) arsitektur jaringan dengan *firewall* untuk mencegah lalu lintas jaringan dari lewat langsung antara jaringan perusahaan dan *SMART GRID*, dan memiliki mekanisme otentikasi terpisah dan mandat untuk pengguna jaringan perusahaan dan *SMART GRID*. *SMART GRID* juga harus menggunakan topologi jaringan yang memiliki beberapa lapisan, dengan komunikasi yang paling penting terjadi pada lapisan yang paling aman dan dapat diandalkan.
- Membatasi akses fisik ke jaringan *SMART GRID* dan perangkat. Akses fisik tidak sah ke komponen bisa menyebabkan gangguan serius fungsi *SMART GRID* ini. Kombinasi kontrol akses fisik harus digunakan, seperti kunci, pembaca kartu, dan/atau penjaga.
- Melindungi komponen *SMART GRID* dari eksploitasi. Ini termasuk pemakaian *patch* keamanan setelah pengujian di sesuai kondisi lapangan; menonaktifkan semua *port* dan layanan yang tidak digunakan; membatasi hak akses *SMART GRID* untuk hanya mereka yang diperlukan sesuai peran masing-masing orang; pelacakan dan pemantauan audit; dan menggunakan kontrol keamanan seperti perangkat lunak antivirus dan integritas

perangkat lunak di mana secara teknis layak untuk mencegah, mendeteksi, dan mengurangi *malware*.

- Mempertahankan fungsi selama kondisi buruk. Hal ini bagaimana merancang *SMART GRID* sehingga setiap komponen kritis memiliki cadangan atau backup komponen. Selain itu, jika komponen gagal, maka harus berhenti dengan cara yang tidak menghasilkan lalu lintas informasi yang tidak perlu pada *SMART GRID* atau jaringan lain, atau tidak menyebabkan masalah lain di tempat lain.

Sistem pemulihan setelah insiden. Insiden yang tak terelakkan dan rencana respon insiden adalah hal penting. Karakteristik utama dari program keamanan yang baik adalah seberapa cepat sistem dapat dipulihkan setelah insiden terjadi.

Menangani keamanan *SMART GRID* sangat perlu organisasi untuk membentuk tim khusus keamanan siber. Program keamanan siber yang efektif untuk *SMART GRID* harus menerapkan strategi yang dikenal sebagai defense-in-depth, lapisan mekanisme keamanan sehingga dampak dari kegagalan dalam satu mekanisme dapat diminimalkan.

A. Peningkatan Keamanan Jaringan SCADA

Penelitian ini mencoba mengembangkan langkah untuk membantu setiap organisasi meningkatkan keamanan jaringan SCADA. Langkah-langkah ini tidak dimaksudkan untuk menjadi preskriptif atau *all-inclusive*. Namun, menangani tindakan penting yang harus diambil untuk meningkatkan perlindungan jaringan SCADA.

Pemerintah pusat memainkan peran kunci dalam melindungi infrastruktur kritis bangsa sebagai bagian dari strategi keamanan dan ketahanan nasional, *smart grid* merupakan salah satu infrastruktur kritis. Dalam memenuhi tanggung jawab tersebut harus dilakukan *assessment* terhadap organisasi terkait jaringan SCADA untuk mengembangkan pemahaman mendalam tentang jaringan SCADA dan langkah-langkah yang diperlukan untuk mengamankan jaringan SCADA E. Nickolov (2005, pp. 105 – 119).

Langkah-langkah terkait teknis dalam upaya peningkatan keamanan jaringan SCADA:

a. Identifikasi semuakoneksi ke jaringanSCADA.

Melakukan analisis risiko menyeluruh untuk menilai risiko dan kebutuhan masing-masing koneksi ke jaringan SCADA. Melakukan analisis secara *komprehensif* terkait setiap koneksi ke jaringan SCADA. Mengidentifikasi dan mengevaluasijenis berikut sambungan:

- Jaringan lokal dan jaringan secara lebih luas seperti WAN atau MAN
- Perangkat internet jaringan nirkabel, termasuk uplink satelit
- Modem atau koneksi dial-up
- Koneksi kemitra bisnis, *vendor* atau badan pengatur atau badan pengawas

b. Koneksi yang tidak perlu segera diputus dari jaringanSCADA.

Untuk memastikan tingkat keamanan tertinggi dari sistem SCADA, mengisolasi jaringan SCADA dari jaringan lain merupakan hal yang masuk akal. Setiap koneksi kejaringan lainyang menimbulkan risiko keamanan harus segera diputus dari jaringan SCADA, isolasi jaringan SCADA harus menjadi tujuan utama untuk memberikan perlindungan yang diperlukan. Strategi seperti pemanfaatan "zona demiliterisasi" (DMZ) dan *data warehousing* dapat memfasilitasi transfer data yang aman dari jaringan

SCADA untuk jaringan bisnis. Namun harus dirancang dan implementasi dengan benar untuk menghindari muncul risiko tambahan melalui konfigurasi yang tidak benar.

c. Mengevaluasi dan memperkuat keamanan koneksi yang tersisa ke jaringan SCADA.

Melakukan pengujian penetrasi atau analisis kerentanan koneksi yang tersisa ke jaringan SCADA untuk mengevaluasi terkait perlindungan pada jaringan tersebut. Hasil pengujian akan menjadi bahan evaluasi untuk manajemen risiko. Ketika terjadi adanya indikasi kelemahan pada jaringan SCADA diharapkan untuk mengimplementasikan *firewall*, sistem deteksi intrusi (IDS/IPS), honeypot untuk SCADA dan langkah-langkah keamanan lain yang sesuai dengan praktisi terbaik. Manajemen organisasi harus memahami dan menerima tanggung jawab atas risiko yang terkait dengan koneksi ke jaringan SCADA.

d. Mempertegas jaringan SCADA dengan menghapus atau menonaktifkan layanan yang tidak perlu.

Server kontrol SCADA yang dibangun di atas sistem operasi komersial atau *open source* dapat terkena serangan melalui layanan jaringan yang masih dalam kondisi setting standar. Hal yang dapat dilakukan yaitu menghapus layanan yang tidak digunakan dan daemon jaringan yang tidak diperlukan untuk mengurangi risiko serangan langsung. Hal ini sangat penting ketika jaringan SCADA saling berhubungan dengan jaringan lain. Jangan membiarkan layanan atau fitur pada jaringan SCADA kecuali penilaian risiko menyeluruh sehingga konsekuensi yang memungkinkan layanan fitur menunjukkan bahwa manfaat dari layanan/fitur jauh lebih besar dari pada potensi eksploitasi kerentanan.

e. Tidak mengandalkan protokol *proprietary* untuk melindungi sistem SCADA.

Beberapa sistem SCADA merupakan unik, protokol *proprietary* yang digunakan untuk komunikasi antara perangkat di lapangan dengan server. Seringkali keamanan sistem SCADA hanya didasarkan pada kerahasiaan protokol ini.

f. Menerapkan fitur keamanan yang disediakan oleh perangkat dan sistem vendor.

Kebanyakan sistem SCADA yang lebih tua (kebanyakan sistem yang saat ini digunakan) tidak memiliki fitur keamanan sama sekali. Pemilik sistem SCADA harus bersikeras bahwa penjual sistem menerapkan fitur keamanan dalam bentuk *patch* atau upgrade produk. Beberapa perangkat SCADA dioperasionalkan dengan fitur keamanan dasar, tapi ini biasanya dinonaktifkan untuk memastikan kemudahan instalasi. Menganalisis setiap perangkat SCADA untuk menentukan apakah fitur keamanan telah tersedia. Selain itu, Pada dunia industri terkait keamanan (seperti *firewall*) sering diatur untuk memberikan kegunaan yang maksimal, tetapi meminimalkan keamanan. Atur semua fitur keamanan untuk memberikan tingkat keamanan maksimum.

g. Menetapkan kontrol yang kuat atas media yang digunakan sebagai *backdoor* ke jaringan SCADA.

Backdoors atau koneksi ke *vendor* memang ada dalam sistem SCADA, otentikasi yang kuat harus dilakukan untuk memastikan komunikasi yang aman. Modem, jaringan nirkabel, dan jaringan kabel digunakan untuk komunikasi dan terkait kebutuhan perawatan merupakan kerentanan yang signifikan

terhadap jaringan SCADA. Serangan "*war dialing*" atau "*war driving*" dapat memungkinkan penyerang untuk memotong semua kontrol dan memiliki akses langsung ke jaringan SCADA atau sumber daya penting. Untuk meminimalkan risiko serangan tersebut, menonaktifkan akses *inbound* dan menggantinya dengan beberapa jenis sistem *callback*.

h. Menerapkan sistem deteksi intrusi secara internal dan eksternal dan membangun 24 jam sehari terkait pemantauan insiden.

Untuk dapat secara efektif menangani serangan siber, membangun strategi deteksi intrusi yang mencakup memperingatkan administrator jaringan terkait aktivitas jaringan berbahaya yang berasal dari sumber internal atau eksternal. Monitoring sistem deteksi intrusi sangat penting dilakukan 24 jam sehari. Selain itu, prosedur penanganan insiden harus berada di lokasi untuk memungkinkan tanggapan yang efektif terhadap serangan apapun. Untuk melengkapi jaringan pemantauan, mengaktifkan *logging* pada semua sistem dan log sistem audit setiap hari untuk mendeteksi aktivitas yang mencurigakan sesegera mungkin.

i. Lakukan audit teknis perangkat SCADA dan jaringan, dan jaringan lain yang terhubung, untuk mengidentifikasi masalah keamanan.

Audit teknis dari perangkat SCADA dan jaringan sangat penting untuk efektivitas keamanan yang sedang berlangsung. Banyak alat-alat keamanan komersial dan *open source* yang tersedia yang memungkinkan administrator sistem untuk melakukan audit sistem/jaringan untuk mengidentifikasi layanan aktif, *patch*, dan kerentanan umum. Penggunaan alat ini tidak akan memecahkan masalah sistemik, tetapi akan menghilangkan lubang keamanan yang memungkinkan seorang penyerang bisa mengeksploitasi. Menganalisis kerentanan yang diidentifikasi untuk menentukan signifikansi, dan mengambil tindakan perbaikan yang sesuai. Melacak tindakan perbaikan dan menganalisa informasi untuk mengidentifikasi tren yang terjadi.

j. Melakukan survei keamanan fisik dan menilai semua situs *remote* yang terhubung ke jaringan SCADA untuk mengevaluasi keamanan.

Setiap lokasi yang memiliki koneksi ke jaringan SCADA adalah target, situs *remote* baik yang tidak terjaga atau terjaga. Melakukan survei keamanan dan akses persediaan titik fisik pada setiap fasilitas yang memiliki koneksi ke sistem SCADA. Mengidentifikasi dan menilai sumber informasi termasuk telepon jarak jauh/jaringan komputer/kabel serat optik yang dapat disadap; radio dan *microwave link* yang dimanfaatkan; terminal komputer yang dapat diakses; dan area akses titik jaringan nirkabel lokal. Keamanan situs harus memadai untuk mendeteksi atau mencegah akses yang tidak sah.

k. Membangun Tim Tanggap Darurat untuk mengidentifikasi dan mengevaluasi skenario serangan.

Membentuk "Tim Tanggap Darurat" untuk mengidentifikasi skenario serangan potensial dan mengevaluasi kerentanan sistem potensial. Tim terdiri dari beberapa individu yang dapat memberikan wawasan tentang kelemahan jaringan secara keseluruhan, sistem SCADA, sistem fisik, dan kontrol keamanan. Orang-orang yang bekerja pada sistem setiap hari melakukan eksplorasi ke

dalam kerentanan jaringan SCADA dan harus dikonsultasikan ketika mengidentifikasi skenario serangan potensial dan konsekuensi yang mungkin. Memastikan bahwa risiko dari penyusup berbahaya harus sepenuhnya dievaluasi, mengingat bahwa ini merupakan salah satu ancaman terbesar bagi sebuah organisasi. Informasi yang dihasilkan dari "Tim Tanggap Darurat" dievaluasi ke dalam risiko dan memproses secara manajemen untuk menilai informasi dan membangun strategi perlindungan yang tepat.

Kontrol Keamanan SCADA

Kontrol keamanan terkait manajemen, operasional, dan kontrol teknis dalam sistem informasi untuk melindungi kerahasiaan, integritas, dan ketersediaan sistem dan informasinya. Panduan untuk memilih dan menentukan kontrol keamanan untuk mendukung sistem informasi infrastruktur kritis. Kontrol keamanan disusun menjadi tiga aspek: manajemen, operasional, dan kontrol teknis Udassin (2008)

a. Kontrol Manajemen

Kontrol manajemen terkait penanggulangan keamanan untuk SCADA berfokus pada manajemen risiko dan pengelolaan keamanan informasi. Aktivitas pada control manajemen antara lain:

- Penilaian keamanan dan otorisasi

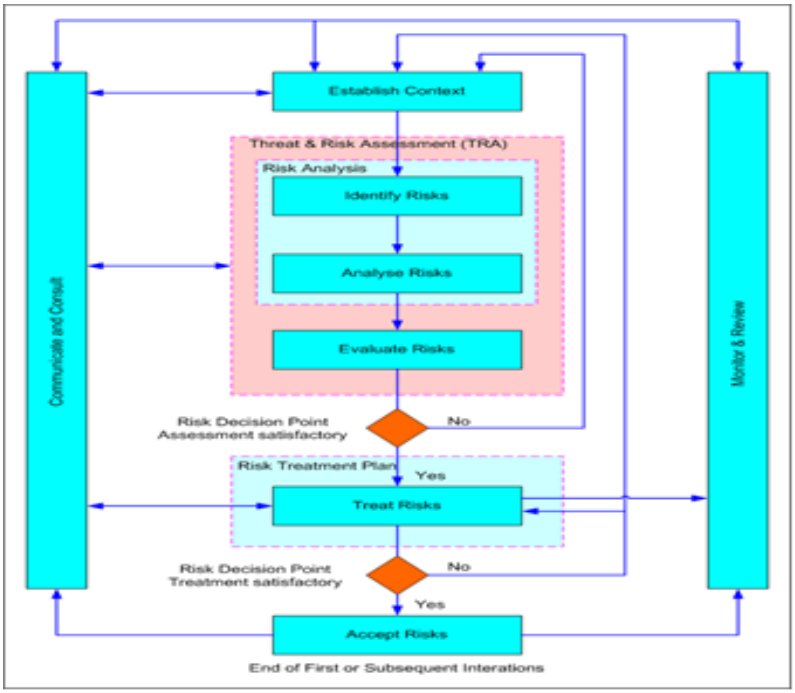
  Kontrol keamanan memberikan dasar untuk melakukan penilaian secara berkala dan memberikan sertifikasi kontrol keamanan yang diimplementasikan dalam sistem informasi untuk menentukan apakah kontrol dilaksanakan dengan benar, operasi sebagaimana dimaksud, dan memproduksi hasil yang diinginkan untuk memenuhi persyaratan sistem keamanan.

- Perencanaan

  Sebuah rencana keamanan merupakan dokumen formal yang memberikan gambaran tentang persyaratan keamanan untuk sistem informasi dan menjelaskan kontrol keamanan di tempat atau direncanakan untuk memenuhi persyaratan. Kontrol keamanan yang termasuk dalam Perencanaan memberikan dasar untuk mengembangkan rencana keamanan. Kontrol ini juga membahas isu-isu pemeliharaan berkala memperbarui rencana keamanan.

- Manajemen Risiko

Manajemen risiko harus dilakukan dengan sistematis sehingga perlu disusun tahapan yang merupakan perwujudan dari alur pemikiran dari tahap definisi masalah, analisa solusi hingga rencana perancangan. Kerangka kerja tersebut merujuk pada kerangka kerja manajemen risiko atau Risk Management Framework (RMF). Kerangka kerja tersebut diatur pada ISO 31000:2009 (*Risk management — Principles and guidelines*). Standar tersebut adalah standar pendukung untuk ISO 31000 dan memberikan pedoman untuk pemilihan dan penerapan teknik sistematis untuk menilai/melakukan assessment risiko The Public Risk Management Association (2010). Versi pertama standar ini diterbitkan pada bulan November 2009. Panduan ini memberikan pendekatan terstruktur untuk menerapkan manajemen risiko secara perusahaan-yang kompatibel dengan kedua COSO ERM dan ISO 31000. Namun, panduan lebih menekankan pada ISO 31000 karena merupakan standar internasional dan banyak organisasi memiliki operasi internasional. Berikut adalah alur proses manajemen risiko yang akan dilakukan dengan mengadaptasi ISO31000:



Gambar 4. Kerangka Kerja Proses Manajemen Risiko

Secara detail alur pengerjaan dijelaskan di bawah ini;

Tahap I : Penentuan Kontek

bertujuan untuk melakukan identifikasi permasalahan. Setelah permasalahan berhasil diidentifikasi selanjutnya mengumpulkan seluruh data obyek studi kasus dan literatur yang terkait. Data tersebut terdiri atas data kualitatif, dokumen pendukung dan literatur yang terkait. Pada tahapan ini juga dilakukan penentuan kontek terkait risiko, mencakup filosofi manajemen risiko di SCADA pada infrastruktur kritis, *risk appetite*, struktur organisasi, matriks RACI (*Responsible, Accountable, Consulted, Informed*).

Tahap II : *Risk Assessment*

Merupakan proses pengembangan manajemen risiko, hal yang dilakukan adalah identifikasi risiko, baik risiko *inherent* maupun risiko residual; Analisis risiko, yang mencakup pemetaan risiko, penghitungan *likelihood* untuk melihat risiko mana saja yang kritikal dan tidak kritikal dan evaluasi risiko.

Tahap III : *Risk Treatment*

Proses penentuan respon terhadap risiko yang ada. Selanjutnya respon-respon yang diidentifikasi, dilakukan filter untuk menentukan respon yang tepat sesuai kontek. Tahap selanjutnya merupakan penentuan kontrol. Diawali dengan penyusunan daftar kontrol, mengintegrasikan antara respons terhadap risiko dengan kontrol, menetapkan kategori kontrol.

Tahap IV : *Information and Communication*

Tahap ini dilakukan untuk menjaga kesesuaian manajemen proses bisnis dengan tujuan dan sasaran strategik. Mekanisme aliran informasi dan komunikasi yang terjadi pada setiap level akan dirancang pada tahap ini.

Tahap V : *Monitoring*

Pada tahap ini dirancang mekanisme *monitoring* dalam implementasi manajemen risiko secara berkala.

- Sistem dan jasa akuisisi

Kontrol keamanan yang termasuk dalam sistem dan jasa akuisisi memberikan dasar untuk mengembangkan kebijakan dan prosedur untuk akuisisi sumber daya yang dibutuhkan untuk cukup melindungi sistem informasi. Akuisisi ini didasarkan pada persyaratan keamanan dan spesifikasi keamanan. Sebagai bagian dari prosedur akuisisi, sistem informasi dikelola menggunakan proses pengembangan sistem metodologi siklus yang mencakup pertimbangan keamanan informasi. Sebagai bagian dari akuisisi, dokumentasi yang memadai harus dipertahankan pada sistem informasi dan konstituen komponen.

- Program Manajemen

  Kontrol keamanan yang termasuk dalam program manajemen fokus pada persyaratan keamanan informasi seluruh organisasi yang independen terhadap sistem informasi tertentu dan sangat penting untuk mengelola program keamanan informasi.

b. Kontrol Operasional

Pengendalian operasional adalah penanggulangan keamanan untuk SCADA yang terutama diterapkan dan dilaksanakan oleh orang-orang dalam sistem, terdiri dari:

- Personil Keamanan: kebijakan dan prosedur untuk posisi personil kategorisasi, skrining, mentransfer, penalti, dan pengakhiran; juga membahas keamanan personil pihak ketiga.
- Perlindungan Fisik dan Lingkungan: kebijakan dan prosedur menangani fisik, transmisi, dan kontrol akses serta kontrol lingkungan untuk pengondisian (misalnya, suhu, kelembaban) dan darurat ketentuan (misalnya, *shutdown*, listrik, pencahayaan, perlindungan kebakaran).
- *Contingency Planning*: kebijakan dan prosedur yang dirancang untuk memelihara atau memulihkan bisnis operasi, termasuk operasi komputer pada lokasi alternatif dalam hal keadaan darurat, kegagalan sistem, atau bencana.
- Manajemen Konfigurasi: kebijakan dan prosedur untuk mengendalikan modifikasi perangkat keras, *firmware*, perangkat lunak, dan dokumentasi untuk memastikan sistem informasi dilindungi terhadap modifikasi yang tidak benar sebelum, selama, dan setelah implementasi sistem.
- Pemeliharaan: kebijakan dan prosedur untuk mengelola semua aspek pemeliharaan sistem informasi.
- Integritas Sistem dan Informasi: kebijakan dan prosedur untuk melindungi sistem informasi dan data dari cacat desain dan modifikasi data menggunakan verifikasi fungsi, integritas data dengan pemeriksaan, deteksi intrusi, deteksi kode berbahaya, dan peringatan keamanan dan kontrol penasihat.
- Perlindungan Media: kebijakan dan prosedur untuk memastikan penanganan yang aman media. Kontrol meliputiakses, pelabelan, penyimpanan, transportasi, sanitasi, penghancuran, dan pembuangan.
- Insiden Respon: kebijakan dan prosedur yang berkaitan dengan pelatihan respon terhadap insiden, pengujian, jasa penanganan, pemantauan, pelaporan, dan dukungan.
- Kesadaran dan Pelatihan: kebijakan dan prosedur untuk memastikan bahwa semua pengguna sistem informasi diberikan pelatihan keamanan yang sesuai relatif terhadap penggunaannya dari sistem dan pelatihan akurat

dengan catatan selalu dipelihara (terdokumentasi).

c. Kontrol Teknis

Kontrol teknis adalah penanggulangan keamanan untuk SCADA yang terutama diterapkan dan dieksekusi oleh sistem melalui mekanisme yang terkandung dalam perangkat keras, perangkat lunak, atau *firmware*dari komponen sistem. Empat jenis pengawasan di kontrol teknis:

- Identifikasi dan Otentikasi: proses verifikasi identitas pengguna, proses, atau perangkat, melalui penggunaan kredensial tertentu (misalnya, kata sandi, token, biometrik), sebagai prasyarat untuk memberikan akses ke sumber daya dalam sistem TI.
- *Access Control*: proses pemberian atau menyangkal permintaan khusus untuk memperoleh dan menggunakan informasi dan jasa pemrosesan informasi terkait untuk akses fisik ke area dalam lingkungan sistem informasi.
- Audit dan Akuntabilitas: kajian independen dan pemeriksaan catatan dan kegiatan untuk menilai kecukupan pengendalian sistem, untuk memastikan kepatuhan dengan kebijakan yang ditetapkan dan prosedur operasional, dan untuk merekomendasikan perubahan yang diperlukan dalam kontrol, kebijakan, atau prosedur.
- Sistem dan Perlindungan Komunikasi: mekanisme untuk melindungi baik sistem dan komponen transmisi data.

Penerapan ISO/IEC 27001:2013 dan ISO/IEC 27004:2009

ISO/IEC 27001:2013 ini mencakup persyaratan untuk *assessment* dan penanganan risiko keamanan informasi yang disesuaikan dengan kebutuhan organisasi. Persyaratan standar ini bersifat umum dan ditujukan untuk diaplikasikan pada semua organisasi tanpa memperhatikan jenis, ukuran, dan sifatnya. Persyaratan yang ditetapkan di klausul 4 sampai 10 wajib dilaksanakan oleh organisasi untuk mendapat kesesuaian terhadap standar ini. Adapun Klausul dalam ISO/IEC 27001: 2013 terdiri dari 7 klausul yaitu:

- Klausul 4 Konteks Organisasi
- Klausul 5 Kepemimpinan
- Klausul 6 Perencanaan
- Klausul 7 Pendukung
- Klausul 8 Operasi
- Klausul 9 Evaluasi Kinerja
- Klausul 10 Peningkatan

ISO/IEC 27004:2009 ini memberikan panduan tentang pengembangan dan penggunaan langkah-langkah dan pengukuran untuk menilai efektivitas diimplementasikan Sistem Manajemen Keamanan Informasi dan kontrol atau kelompok kontrol, sebagaimana ditentukan dalam ISO / IEC 27001:2013.

PENUTUP

Penerapan system manajemen keamanan informasi pada SCADA di power grid dapat menggunakan Standar yang mengacu pada ISO/IEC 27001:2013 (*Information Security Management System*). Disamping itu untuk penerapan prinsip manajemen risiko juga dapat mengacu pada Risk Management Framework (RMF), ISO31000:2009 (Risk management — Principles and guidelines). Proses yang dilakukan terdiri atas: penentuan context, penilaian risiko dan perlakuan risiko. Komponen lain yang tidak dapat dipisahkan dalam proses manajemen risiko adalah komunikasi, konsultasi, monitoring dan review.

Proses yang dilakukan terdiri atas: penentuan context, penilaian risiko dan perlakuan risiko. Komponen lain yang tidak dapat dipisahkan dalam proses manajemen risiko adalah komunikasi, konsultasi, monitoring dan review. Penentuan konteks risiko dapat diturunkan dari aset yang dimiliki oleh organisasi dan terkait dengan proses bisnis sistem SCADA. Penilaian risiko dilakukan bertujuan untuk menghasilkan daftar risiko, analisis dan evaluasi risiko yang ada. Perlakuan risiko ditentukan sebagai langkah terakhir yang diambil untuk menangani dampak dan kemungkinan terjadinya risiko yang telah diidentifikasi sebelumnya. Proses-proses tersebut merupakan langkah-langkah terstruktur dan berkelanjutan dalam penerapan manajemen risiko untuk SCADA pada power grid.

Terkait kebijakan pengamanan infrastruktur system elektronik dengan kategori kritis (*critical information infrastructure*), perlu dibuatkan kebijakan Pengamanan Infrastruktur sistem Elektronik yang merujuk pada Kerangka Kerja Manajemen Risiko, ISO IEC 31000 dan juga Sistem Manajemen Keamanan Informasi, ISO/IEC 27001:2013.

Berdasarkan hasil penilaian kondisi saat Tata Kelola Keamanan Informasi yang telah dilakukan, dapat diberikan rekomendasi kepada semua pihak Perusahaan sebagai berikut:

1. Konteks Organisasi: Perusahaan harus menentukan isu-isu eksternal dan internal yang relevan dengan pencapaian tujuan organisasi dan menentukan pihak yang terkait dengan Keamanan Informasi Pemerintahan serta untuk mengembangkan, mengoperasikan, memelihara, dan meningkatkan suatu Tata Kelola Keamanan Informasi berkelanjutan.
2. Konteks Kepemimpinan: Memastikan kebijakan dan tujuan Tata Kelola dan Keamanan Informasi telah disusun sesuai dengan arah kebijakan strategis organisasi dan memastikan integrasi proses Tata Kelola Keamanan Informasi ke dalam proses bisnis organisasi.
3. Perencanaan Konteks: Perusahaan perlu merencanakan bagaimana mengintegrasikan, melaksanakan, dan mengevaluasi tindakan apapun proses Tata Kelola Keamanan Informasi melalui proses penilaian risiko dan mitigasi risiko.
4. Konteks Dukungan: Perusahaan harus menetapkan dan menyediakan sumber daya yang diperlukan dalam penyusunan, pelaksanaan, pemeliharaan dan peningkatan Tata Kelola Keamanan Informasi berkelanjutan
5. Konteks Operasional: Perusahaan harus menerapkan dan proses kontrol yang diperlukan sesuai dengan ketentuan Tata Kelola Keamanan Informasi dan melaksanakan rencana manajemen risiko keamanan informasi.
6. Konteks Evaluasi Pelaksanaan: Perusahaan perlu melakukan audit internal pada periode perencanaan untuk memberikan informasi tentang Tata Kelola Keamanan Informasi dan peninjauan Tata Kelola Keamanan Informasi Pemerintahan pada periode perencanaan untuk memastikan keberlanjutan, kecukupan dan efektivitas

Peningkatan Konteks: Perusahaan harus melakukan perbaikan Tata Kelola Keamanan Informasi secara berkelanjutan oleh tepat, memadai, dan efektif.

Ini akan mencakup kebijakan, manajemen risiko keamanan informasi, tujuan pengendalian, kontrol,

proses dan prosedur, dan mendukung proses revisinya, membantu untuk menentukan apakah salah satu proses Sistem Manajemen Keamanan Informasi atau kontrol perlu diubah atau diperbaiki. Perlu harus diingat bahwa tidak ada pengukuran kontrol dapat menjamin keamanan yang lengkap. Implementasi pendekatan ini merupakan suatu program ukuran Keamanan Informasi yang akan membantu manajemen dalam mengidentifikasi dan mengevaluasi proses Sistem Manajemen Keamanan Informasi apakah *non-compliant* dan tidak efektif dan memprioritaskan tindakan yang terkait dengan perbaikan atau mengubah proses-proses dan/atau control.

UCAPAN TERIMA KASIH

Peneliti mengucapkan terima kasih kepada pihak-pihak yang telah membantu dalam menyelesaikan penelitian ini. Kuskridho A, yang selalu memberi masukan, serta Syarifuddin yang membantu dalam penelitian sebagai coder pada proses analisis data

DAFTAR PUSTAKA

A.A.S.S.M. G. Adam Hahn.(2013).*Cyber-Physical Security Test beds: Architecture, Application,and Evaluation for Smart grid*.IEEE.

Badan Standardisasi Nasional.(2009).*SNI ISO/IEC 27004:2009*.Jakarta: Badan Standardisasi Nasional.

Badan Standardisasi Nasional.(2013).*SNI ISO/IEC 27000:2013:Sistem manajemen keamanan informasi-Gambaran*.Jakarta: Badan Standardisasi Nasional.

Badan Standardisasi Nasional.(2013).*SNI ISO/IEC 27002:2013:Panduan praktik manajemen keamanan informasi*.Jakarta:Badan Standardisasi Nasional.

C.M.R.B.B.W. H. Saman Zonouz.(2014).SOCCA:A *Security-Oriented Cyber-Physical Contingency Analysis in Power Infrastructures*.IEEE.

C.Scott.(2014).*Designing and Implementing a Honeypot for a SCADA Network*.SANS Institute.

C.T.Wibowo.(2013).*Modul Pelatihan PLC - SCADA*.Universitas Gadjah Mada.

Cyberoam.(2013).*Protecting Critical Infrastructure with Cyberoam's Holistic Security*. Cyberoam.

E.H Gary J. Finco.(2006).*Introduction SCADA Security for Managers and Operators*.SANS SCADA Security Summit II.

E.Nickolov.(2005).*Critical information infrastructure protection: analysis, evaluation and expectations. Information & Security*. AAN International Journal,17, 105-119.

E. Udassin.(2008).*Control System Attack Vectors And Examples*: Field Site And Corporate Network.C4 Security.

Federal Energy Regulatory Commission.(2013).*Critical Infrastructure Protection Reliability Standards*. Federal Energy Regulatory Commission-USA.

G. Seifert.(2013).*CyberSecurity Basics on securing your data*.Federal Solutions Architect OSIsoft.

ISO/IEC.(2013).ISO/IEC 27002:2013.ISO/IEC.

ISO/IEC.(2013)ISO/IEC 27001:2013, ISO/IEC, .

ISO/IEC.(2014).ISO/IEC 27000:2014.ISO/IEC.

J. F. K. S. Keith Stouffer.(2011). *NIST Special Publication 800-82 Guide to Industrial Control Systems (ICS) Security*.NIST.

J. S. Sauver.(2004).*SCADA Security*. Niversity of Oregon Computing Center.

J.W.Cresswell.(2008).*Research Design: Qualitative, Quantitative, and Mixed Methods Approaches, Third Edition*.SAGE Publications.

J.Z.Christian Paulino.(2012).*SCADA Security Example*.Florida Gulf Coast University.

K.G.X.Z.T.Z. Xiao Liang.(2013).*A Study on Cyber Security of Smart grid on Public Networks*.IEEE.

K.M.L.S. L.B.P.H.Y. Yang.(2014).*Multiattribute SCADA-Specific Intrusion Detection System for Power Networks*.IEEE.

K.Zedda.(2010).*New generation of Secure SCADA allowing for intelligent threat monitoring*.ARTEMIS Industry Association.

M.Hendrson.(2007).*Protecting Critical Infrastructure from Cyber Attacks*. Department of Homeland Security-USA.

M.Ko.,C.Dorantes.(2006).*The impact of information security breaches on financial performance of the breached firms: an empirical investigation.* Journal of Information Technology Management, XVII, 13-22.

M. Rydell. (2009).*SCADA Security*. University of Texas at San Antonio.

M.Winanda.(2014).*Keamanan Pengiriman Data Pada Smart grid Untuk Grid Tegangan Tinggi Antar Gardu Induk*.STEI ITB.

National Institute of Standard and Technology(2007).*NISTIR 7628 Guidelines for Smart grid Cyber Security*.*Smart grid* Interoperable Panel (SGIP) Cyber Security Working Group. NIST – U.S. Department of Commerce.

National Institute of Standard and Technology.(2010).*NIST Framework and Roadmap for Smart grid Interoperability Standard*, Rel. 1.0.NIST-U.S. Department of Commerce.

P.A.Metin Ozturk.(2011).*SCADA Security*: Challenges and Solutions.Schneider Electric.

P.J.H.S.P.V.R.P.K.G.B.W.Pitt Turner IV.(2008).*Tier Classications Dene Site Infrastructure Performance*.Uptime Institute.

S. G. A. D. W. P. S. Jonathan Kirsch, *Survivable SCADA Via Intrusion-Tolerant Replication*," IEEE, 2014.

The Public Risk Management Association, *A Structured Approach to Enterprise Risk Management (ERM) and the requirements of ISO 31000*, AIRMIC, The Institute of Risk Management, 2010