تکنیک های خلاقیت گروهی برای امنیت سیستم های اسکادا و اتوماسیون پست

پدیده نوبخت

شرکت برق منطقه ای خراسان، مشهد،
Padideh.nobakht@gmail.com

چکیده

به دلیل وجود مزیت های بسیار زیاد شبکه های هوشمند در آینده نزدیک این شبکه ها جایگزین شبکه های قدرت کنونی می شوند. حرکت به سمت مکانیزه کردن فرایند مدیریت در شبکه قدرت با استفاده از زیر ساخت های IT نقطه عطف در شبکه های قدرت خواهد بود. همانطور که می دانیم استفاده از IT با وجود مزایای بسیار زیاد تهدید های جدی را نیز به همراه خواهد داشت. بنابراین کاربران باید تمام الزامات امنیتی را شناسایی و تا حد امکان اقدامات امنیتی مربوط به آنها را رعایت نمایند. از آنجایی که اقدامات امنیتی شبکه های هوشمند حتی از اقدامات امنیتی مربوط به حساب های مشترکین بانکی مهم تر می باشد کاوش های مربوط به این الزامات نیز باید دقیق تر و موشکافانه تر باشد. بنابراین نیاز به روش های نوین جهت شناسایی الزامات امنیتی می باشد. از طرفی ترکیب رشته ها راهکار های مناسب تری را در اختیار پژوهشگران قرار می دهد در این مقاله به معرفی روش ترکیبی برای داده کاوی و کشف اقدامات امنیتی سیستم های اسکادا پرداخته شده است.

کلمات کلیدی

پروتکل؛ امنیت سایبری؛ حمله ؛ توفان ذهنی؛ تکنیک گروهی.

۱- مقدمه

روش هایی که تا کنون برای امنیت سیستم های اسکادا ارائه شده است بر اساس مطالعه استاندارد های موجود، راهکار های ارائه شده توسط سازندگان تجهیزات، درس آموخته های پروژه های قبلی و کتب و مقالات ارائه شده می باشد. با توجه به اینکه مسئولیت پیاده سازی سیستم های اسکادا به عهده شرکت های برق منطقه ای می باشد و پایگاه متمرکزی برای دریافت درس آموخته های پروژه های قبلی وجود ندارد، امکان استفاده از تجارب سایر شرکت های داخلی و خارجی به صورت متمرکز وجود ندارد. از طرفی اکثر تجهیزات مخابراتی و خصوصا پروتکل های صنعت برق غیر بومی می باشند و سازندگان خارجی کلیه اطلاعات را در اختیار خریداران قرار نمی دهند. بنابراین نه تنها شناخت کامل از طریق سازندگان برای خریداران به وجود نمی آید که ممکن است سازندگان خود یک تهدید باشد و در زمان مناسب به سیستم حمله کند. با بررسی استاندارد ها، مقالات و کتب منتشر شده به این نتیجه رسیدیم که الزامات امنیتی تعریف شده در شبکه های هوشمند هنوز در ابتدای راه می باشند و نیاز به بازنگری و تحقیقات بیشتری دارند. بنابراین باید راه حل های بهتری برای امنیت این شبکه ها جستجو کرد. با استفاده از روش ها و تکنیک های گروهی که در استاندارد های مدیریتی مانند PMBOK مطرح شده است توانایی استفاده از خلاقیت ذهن افراد فراهم می شود. در صورت استفاده از متخصصین صنعت برق کشور، اساتید دانشگاه و محققین کشور و با استفاده از این روش ها امکان رسیدن به راه حل های بهینه وجود دارد. روشی که در این مقاله استفاده شده است ترکیبی از روش توفان ذهن و تصمیم گیری گروهی را معرفی می کند. به نظر می رسد استفاده از این روش در سطح کشور و با ترکیبی که در بالا ذکر شد نتایج بسیار علمی وارزشمندی را به همراه خواهد داشت. همچنین ایجاد یک پایگاه داده اختصاصی برای کاربران خاص و ثبت درس آموخته های قبلی و نتایج حاصل از تکنیک های خلاقیت گروهی مربوط به امنیت این سیستم ها کمک زیادی به امنیت شبکه قدرت می کند. برگزاری جلسات الکترونیکی باعث افزایش بهره وری خواهد شد.

۲- معرفی روش توفان ذهنی[۱]

توفان فکری فرآیندی است که در بسیاری از سازمان‌ها در جهت پیشنهادگیری از کارکنان استفاده می‌گردد. دلیل موفقیت این روش آن است که افراد به جای آنکه توانایی‌های تحلیلی و قضاوتی خویش را بکار

ببندند، استعدادهای خلاقه خود را به خدمت می‌گیرند و از این طریق تعداد زیادی ایده و پیشنهاد از گروهی از افراد در زمان کوتاه حاصل می‌شود. در فرآیند توفان فکری تولید ایده‌های خوب مورد نظر نیست بلکه هدف تولید تعداد زیادی ایده است که در بین آنها ممکن است ایده‌های غیرمنطقی نیز وجود داشته باشد. در فرآیند توفان فکری تمام ایده‌ها مورد قبول هستند و در این مرحله ایده‌یابی به هیچ وجه مورد قضاوت قرار نمی‌گیرند. این روش دارای مزایا و ویژگی‌های زیادی است که بسیاری از تکنیک‌های دیگر منشعب از این روش است. بعد مهم در فرآیند توفان فکری، تجمع گروهی از افراد است که معمولاً حدود ۱۲ الی ۱۶ نفر می‌باشند. با این تعداد هر نفر امکان ارایه نظرات خود را دارد. همچنین بهتر است تعداد افراد بیش از بیست نفر نباشند چون همه نمی‌توانند به راحتی و در لحظه مناسب ایده خود را بیان کنند و ممکن است رفته رفته اشتیاق خود را از دست بدهند[1].

۲-۱- مراحل توفان فکری

برای انجام توفان فکری نیاز است موارد ذیل انجام گردد:

بیان مشکل: قبل از شروع جلسه توفان فکری تمام شرکت‌کنندگان بایستی از جزئیات مشکل آگاه باشند

بررسی مشکل: در این مرحله کلیه شرکت‌کنندگان باید وجوه مختلف مسأله را درک نمایند و به خوبی برای شروع جلسه آماده باشند.

انتخاب نقطه شروع: در این مرحله تعابیری درباره مشکل به عنوان نقطه آغاز انتخاب می‌شود.

جلسه تمرین: برای آمادگی شرکت‌کنندگان در جلسه و ایجاد تحرک در آنها، لازم است حدود پنج دقیقه جلسه تمرین به اجرا درآید.

شروع جلسه: در این حالت به دو طریق ایده‌های افراد را جمع‌آوری می‌کنند، یکی به طریق کتبی، که افراد نظرات خود را می‌بایست بر روی برگه بنویسند و وقتی هر برگه پر شد آن را بر روی دیوار نصب می‌کنند تا همه آن را مشاهده نمایند. روش دوم ابراز ایده از طریق بیان شفاهی می‌باشد که افراد به ترتیب نظرات و پیشنهادهای خود را ارایه می‌نمایند.

پایان جلسه: وقتی که مسئول جلسه متوجه شود دیگر ایده جدید ارائه نمی شود و افراد در حال خستگی می‌باشند، می‌تواند جلسه را به پایان برساند. تجربه نشان داده است در زمان حدود بیست دقیقه بیش از هشتاد ایده ارایه می‌گردد.

ارزیابی ایده ها: در این حالت کلیه ایده ها مورد ارزیابی قرار می گیرد

۲-۲- قوانین حاکم بر روش توفان فکری

هیچ انتقادی نباید از هیچ ایده‌ای صورت پذیرد. در پایان جلسه ارزیابی از پیشنهادها صورت خواهد پذیرفت.

در یک جلسه توفان فکری تمام اعضا باید جسارت و شهامت اظهار نظر پیدا کرده باشند و بدون ترس از ارزیابی بتوانند پیشنهاد خود را بیان نمایند.

بر دستیابی به حداکثر تعداد نظرات تاکید می‌شود زیرا هرچه تعداد پیشنهادها بیش‌تر باشد احتمال وجود نظرات مفید و ارزشمند بین آنها بیش‌تر می‌شود.

همه چیز یادداشت می‌شود، حتی موارد تکراری و همه نظرات تکوین می‌یابند و هیچ چیز رد نمی‌شود. اعضا می‌توانند علاوه بر ارایه پیشنهاد نسبت به بهبود پیشنهاد خود اقدام نمایند.

۲-۳- اهداف امنیتی

نحوه دسترسی مهاجم به سیستم، اصول امنیتی در برابر تهدیدها و سطوح اطمینان یک سیستم برای رسیدن به اهداف امنیتی مربوطه از دیدگاه های عمده در تعریف امنیت است. محرمانه بودن اطلاعات، صحت اطلاعات، دسترس پذیری اطلاعات، تصدیق هویت، مجوز، قابلیت ممیزی و بازرسی، عدم انکار و حفاظت در مقابل شخص ثالث به عنوان هدف های امنیتی قابل استفاده در سیستم هستند.

۳- معرفی روش تصمیم گروهی[2]

تصمیم گیری گروهی فرآیند ارزیابی گزینه های مختلف موجود با نتیجه مورد انتظار می باشد، بطوریکه مشکلات آتی رفع گردد. این تکنیک می تواند در تولید، طبقه بندی و اولویت بندی الزامات محصول، استفاده گردد.

روش های تصمیم گیری گروهی شامل موارد ذیل است:

اتفاق نظر: همه با یک راهکار موافق هستند

اکثریت : بیشتر از ۵۰ درصد از اعضای گروه موافق اند

چند دستگی : بزرگترین دسته در گروه تصمیم گیری می کند

دیکتاتوری: یک فرد برای گروه تصمیم می گیرد

۴- روش انجام کار

در این تحقیق عنوان موضوع را امنیت سیستم اسکادا و اتوماسیون پست تعریف کردیم. سپس منابع مرتبط با موضوع بررسی شد. پس از بازدید از مراکز دیسپاچینگ، پست های فوق توزیع و انتقال و زیر ساخت های

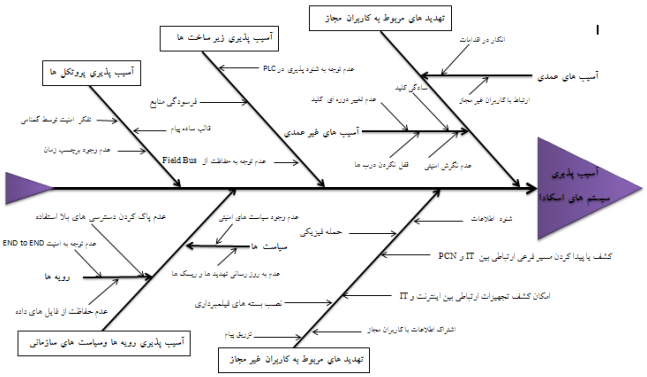
مخابراتی ومذاکره با بهره برداران سیستم، مشاورین و پیمانکاران تهدید ها و ریسک های به شرح ذیل شناسایی شد:

- سیاست ها و رویه های سازمانی،
- کاربران غیر مجاز
- کاربران مجاز
- زیر ساخت‌های مخابراتی
- پروتکل‌ها

پس از شناسایی ریسک‌های کلان اقدامات ذیل انجام شد:

- ثبت موضوع مساله با عنوان آسیب پذیری سیستم های اسکادا به عنوان موضوع اصلی(سر ماهی)
- طرح عوامل، آسیب ها و ریسک های اصلی مساله
- چیدن مسائل ساده تر در نزدیکی موضوع اصلی(سر ماهی) و مسائل پیچیده تر با فاصله از موضوع اصلی(دم ماهی)
- ایجاد عوامل زیر مجموعه ذیل عوامل اصلی
- بررسی تمامی علت های احتمالی وارد شده روی نمودار علت - معلول و متمایز کردن علت هایی که به نظر می رسد تاثیرات بیشتری روی معلول دارند
- شناسایی علت های واقعی براساس مستندات ومدارک صحیح و دقیق (آمار و اطلاعات)
- درج شماره منبع کنار علت هایی که دارای منبع می باشد
- بررسی همبستگی بین علت ها و معلول ها
- حذف موارد قابل حذف و تهیه نمودار نهایی

شکل یک ریسک‌های پروژه را با نمودار استخوان ماهی نشان می‌دهد.



شکل(۱): ریسک‌های پروژه

برای تعریف اقدامات امنیتی مراحل ذیل انجام شد:

- ارسال عنوان موضوع جلسه برای حداکثر ۱۶ نفر از متخصصین و کارشناسان خبره سازمان
- مطالعه تخصصی و تحقیق اینترنتی توسط افراد در رابطه با موضوع جلسه
- شروع جلسه به صورت شفاهی با طرح عنوان الزامات امنیتی شبکه اسکادا
- دریافت و ثبت ایده ها توسط دبیر جلسه
- اعلام خاتمه جلسه در صورت عدم دریافت ایده جدید
- دسته بندی ایده ها و مقایسه ایده ها با استاندارد ها و منابع موجود و ذکر نام منبع
- تشکیل جلسه ارزیابی ایده ها و طرح موارد دسته بندی شده در جلسه
- تهیه لیست نهایی بر اساس تکنیک تصمیم گیری گروهی اکثریت آراء

۵- نتایج حاصل از روش توفان ذهنی

پس از دریافت نظرات در جلسه توفان ذهنی و تهیه لیست نهایی الزامات امنیتی در جلسه تصمیم گیری بر اساس اکثریت آرا اقدامات امنیتی به شرح ذیل دسته بندی می گردد:

۵-۱- اقدامات امنیتی مربوط به کاربران مجاز

- انتخاب کلمه عبور و کلید پیچیده و با طول مناسب و اختصاصی[۴،۱۳]
- تغییر دوره ای کلمه عبور و کلید[۱۳]
- ممنوعیت در استفاده از CD و flash memory و لپ تاپ در مراکز اسکادا و سیستم های متصل به اتوماسیون پست ها
- عدم نصب نرم افزار های موجود در اینترنت و open-source [۱۲]
- کنترل دسترسی کاربران به مناطق مجاور (مثل اینترنت)[۵]
- ذخیره اطلاعات مهم توسط حافظه ها یا سیستم های اختصاصی
- قفل کردن درب ها و کنترل رفت و آمد افراد توسط نگهبان [۱۳]
- استفاده از تجهیزات امنیتی [۱۳]
- پاک کردن نرم افزار های بلا استفاده از سیستم کامپیوتری
- به روز رسانی و استفاده مرتب از نرم افزار ویروس یاب[۴،۶،۱۴]
- جلوگیری از انکار توسط امضاء دیجیتال [۳،۴]

۵-۲- اقدامات امنیتی مربوط به کاربران غیر مجاز

- حفاظت و حراست فیزیکی از مراکز اسکادا
- استفاده از رمز نگاری برای جلوگیری از شنود

۵-۳- اقدامات امنیتی رویه ها و سیاست های سازمانی

- استفاده از DCOM و OPC [4]
- توجه به حد اقل امتیاز دسترسی ها و مدیریت مجوز ها[3,4,6]
- کنترل هویت و ارتباطات کاربران
- استفاده از PKI کامل با لیست ابطال کلیدی [4,6]
- دقت در امنیت پروسه تولید، ارسال و نگهداری کلید

- کنترل و نظارت بر بسته ها
- وجود سیاست های امنیتی و به روز رسانی آن
- به روز رسانی تهدید ها و ریسک ها و مقابله های مورد نیاز
- ایجاد تعادل در اقدامات امنیتی در سیستم وتوجه به آسیب پذیری در برابر لینک ضعیف[4]
- توجه به امنیت END to END[4,15]
- شناخت نوع و انگیزه مهاجمین و به روز رسانی لیست مذکور
- ایزوله کردن شبکه اتوماسیون از شبکه ادری
- ایجاد آلارم ها، اخطار رخداد ها، مبادله داده برای ارتباط سرور به سرور در شبکه های اترنت
- نظارت امنیتی هنگام تعمیر و نگهداری[5]
- ایجاد ممیزی در سیستم[4]
- توجه به درستی اطلاعات با حفاظت در برابر ویرایش های غیر مجاز یا تخریب اطلاعات
- رعایت امنیت سیستم در طراحی، اجرا و بهره برداری پروژه ها[4]
- توجه به غیر فعال کردن سرویس های بلا استفاده[18]
- وجود تفکر آموزش الزامات امنیتی به پرسنل
- حفاظت از فایل های داده در مواقع نیاز[19]
- استفاده از استاندارد IEC 62351 و سایر استاندارد های امنیتی و به روز رسانی استاندارد ها [6,13]
- استفاده از گواهی نامه های پشتیبان[6]
- مدیریت سیاست های امنیتی سرور وکنترل هویت سرور[4,14]

۵-۴- اقدامات امنیتی مربوط به زیر ساخت ها

- استفاده از استاندارد IEEE802.11 برای LAN [۴]
- استفاده از استاندارد IEEE 802.1Q برای VAN[۴]
- استفاده از رمز نگاری در کانال های PLC [۴،۱۱]
- استفاده از رمز نگاری برای حفاظت از Field Bus[۴،۱۱،۷]
- احراز هویت در مکالمه ها در PSTN[۴]
- استفاده از مودم امن [۵]
- ارتباطات امن خارج از سیستم پروتکل انتقال متن ترکیبی امن، VPN و...[۶،۷،۱۱]
- استفاده از WAN / LAN با محدوده مشخص و کنترل زیر بنایی سخت(عوامل انسانی) [۶]
- برقراری ارتباطات اترنت روی SDH[۶]
- تعویض منابع فرسوده[۱۳]
- حفاظت بخش های نا امن شبکه اسکادا توسط دیوار های آتش[۴،۵،۷]
- استفاده از NTP(پروتکل زمان شبکه) و IEEE 1588 جهت سنکرون سازی درخواست های ارسالی به مرکز کنترل[۱۴]
- استفاده از سخت افزار های ایمن[۴]
- دفاع عمیق[۴]
- استفاده از توابع Routing / L3[۶]
- عدم استفاده از تجهیزات بی سیم استاندارد b۸۰۲،۱۱درشبکه های کنترل و صنعتی [۷]
- کنترل صحت تجهیز و سیستم مانند کنترل موارد دانسته(پین کد، کلمه عبوریا کلید رمز نگاری)،داراییها(کلید، کارت هوشمندو dongle[۷]
- حفاظت فیزیکی از تمام تجهیزات گذرگاه که با تجهیزات بیرونی ارتباط دارند [۱۱]
- اولویت دهی IEEE 802.1p در سوئیچ های LAN و اولویت دهی بر پایه IP در روتر ها[۱۴]
- حفاظت تمام ارتباطات بی سیم به وسیله امکانات امنیتی موجود مثل پروتکل های رمز نگاری داده IEEE802.11i with AES [۱۴]
- استفاده از تجهیزات شناسایی و تشخیص نفوذ (IDS) [۴،۵،۶،۷،۹،۱۱،۱۴]

۵-۵- الزامات امنیتی مربوط به پروتکل ها

- استفاده ازپروتکل های WS-security، PGP/GnuPG، S/MIME، HTTP و MMS در لایه کاربردی پروتکل ها[۴]
- استفاده از SSH و SSL/TLS در لایه انتقال پروتکل[۴،۱۲]
- استفاده از IPSec در لایه اینترنت پروتکل ها[۴]
- استفاده از CHAP/PAP، Bluetoth وWEP/WPA/802.1xدر لایه لینک پروتکل ها[۴]
- در نظر گرفتن برچسب زمانی در پیام
- ایجاد اولویت در پیام ها
- استفاده از امضاء دیجیتال ، توابع یکطرفه در رمز نگاری پیام ها[۴،۱۷]
- مدیریت کلید در جلسه[۱۵،۱۶]
- عدم استفاده از پروتکل های باز TCP/IP/Ethernet در اتوماسیون صنعتی LAN
- فعال کردن تصدیق سرور و مشتری[۴]
- فعال کردن مهلت جلسه و شروع مذاکره مجدد[۴]
- ایجاد محدودیت در تعداد ورود هر جلسه[۴]
- حفاظت بر روی پروتکل های مانند SNMP / UDP برای پیکربندی سوئیچ و روتر و SNTP / UDP برای انتقال زمان
- پیاده سازی امنیتی در تمام لایه های پروتکل ها
- استفاده از switchboard [۲۰]

- استفاده از مکانیزم چالش/ پاسخ مورد استفاده در MAC با تصدیق یکطرفه و دو طرفه در [۱۵]ISO/IEC 9798-4
- ساخت پروتکل بومی و ایجا اقدامات امنیتی متناسب با آن
- استفاده از عاملیت و توپولوژی افزونه شامل دو لایه توپولوژی شبکه با RSTP (پروتکل زیر گراف سریع) در پست LAN(شبکه محلی) وOSPF (نوعی پروتکل مسیر یابی با انتخاب کمترین تعداد hop) روی اینترانت و VRRP (پروتکل افزونگی روتر مجازی)برای دسترسی مضاعف به IP شبکه و لینک های پشتیبان بین روتر ها [۱۴]

۶- نتیجه گیری

با استفاده از تکنیک های خلاقیت و تصمیم گیری گروهی امکان تعریف اقدامات امنیتی مورد نیاز سیستم های اسکادا فراهم می شود. این روش از نادیده گرفتن برخی اقدامات امنیتی جلوگیری می کند. همچنین روشی برای ترویج و آموزش امنیت بین پرسنل متخصص می باشد. این روش خود یک کارگاه آموزشی برای انجام کار گروهی و استفاده از تجارب دیگران است. همچنین باعث تشویق مطالعه بیشتر کارشناسان خبره در زمینه های امنیت یا سایر زمینه ها می گردد. با استفاده از روش مذکور و دعوت از متخصصین و پژوهشگران در سطح کشور و کنترل استاندارد ها و مقالات متعدد بخش اعظم اقدامات امنیتی شبکه های هوشمند پوشش داده می شود و باعث ایجاد راه حل های خلاق گروهی می شود. سایر موارد مورد نیاز اقدامات امنیتی نیاز به پژوهش و تحقیق و ارائه راه حل های جدید دارد. همچنین با توجه به الزامات شبکه های قدرت استفاده از روش های رمز نگاری با زمان پردازش کمتر جزء اولویت های اصلی در سیستم های اسکادا می باشد. بنابراین پیشنهاد می شود در تحقیقات بعدی به معرفی روش های رمز نگاری داده ها با ذکر زمان مورد نیاز برای پردازش و مشخصات تجهیزات پردازش گر رمز نگاری پرداخته شود. همچنین در صورت طراحی تجهیزات مخابراتی و پروتکل های اسکادای بومی طراحی روش رمز نگاری بومی متناسب با پروتکل ها و تجهیزات بومی ضروری به نظر می رسد.

مراجع

[1] http://old.ido.ir
[2] Project Management Body Of Knowledge
[3] Daniel E. Nordell, PE, “Communication System Characteristics Part 2”,d.nordell@ieee.org
[4] Dacfey Dzung, Martin Naedele, Thomas P. Von Hoff, Mario Crevatin , “Security for Industrial Communication Systems, ”
[5] “CYBER SECURITY IN SUBSTATION AUTOMATION :DESIGN AND SUPERVISION"،
[6] F. Hohlbaum, P. Schwyter, F. Alvarez ,“Cyber Security requirements and related standards for Substation Automation Systems"
[7] “Technical Information PROFIBUS-PA"،www.samson.de
[8] “PROFINET Security Guideline " ،Order No: 7.002،www.profibus.com
[9] Giovanni A. Cagalaban, Yohwan So, Seoksoo Kim, “SCADA Network Insecurity: Securing Critical Infrastructures through SCADA Security Exploitation" ،
[10] Lynn August Linse , “Implementing Modbus/TCP Avoiding Multi-Vendor Pitfalls ،" ،http://www.iatips.com
[11] Eric J. Byres ،Matthew Franz and Darrin , Miller ,“The Use of Attack Trees in Assessing Vulnerabilities in SCADA Systems "
[12] Gemma Sánchez, Isabel Gómez, Joaquín Luque, Jaime Benjumea, Octavio Rivera, “Using Internet Protocols to Implement IEC 60870-5 Telecontrol Functions
[13] “IEC TC57 WG15:IEC 62351 Security Standards for the Power System Information Infrastructure "،Frances Cleveland,WG15 Convenor Xanthus Consulting International،ver 14
[14] Farkhod Alsiherov, Taihoon Kim , “Research Trend on Secure SCADA Network Technology and Methods "
[15] “SECURE AUTHENTICATION" ،Copyright © 2010 IEEE.
[16] Dong Jin ،David M. Nicol،Guanhua Yan ,“AN EVENT BUFFER FLOODING ATTACK IN DNP3 CONTROLLED SCADA SYSTEMS"
[17] Dae-Yong Shin, Sugwon Hong, Il Hyung Lim, Seung-Jae Lee , “Evaluation of Security Algorithms for the SCADA System based on IEC 61850 "
[18] “Security in the smart grid" ،ABB white paper
[19] “Cyber Security for Protection Related Data Files Report to the IEEE PSRC Main Committee from WG H-18"
[20] “Security Considerations in SCADA Communication Protocols " ،Intelligent Systems Research Laboratory ،Technical Report TR-ISRL-04-01