تحلیل مخاطرات امنیتی یک ایستگاه انتقال، مبتنی بر سیستم اتوماسیون ABB و پروتکل ۶۱۸۵۰

محمدعلی هرمزی[۱]، محمد کریم جمشیدی [۲]، مهدی حیدرنیا[۳] ،محمد رضا پزشکیان[۴]

[۱] مجری طرح اتوماسیون ایستگاه، شرکت برق منطقه ای فارس، شیراز، Mohammadalihormozi56@gmail.com

[۲] کارشناس طرح اتوماسیون ایستگاه، شرکت برق منطقه ای فارس، شیراز، Jamshidim@frec.co.ir

[۳] کارشناس طرح اتوماسیون ایستگاه، شرکت برق منطقه ای فارس، شیراز، Mehdi.he0917@gmail.com

[۴] کارشناس طرح اتوماسیون ایستگاه، شرکت برق منطقه ای فارس، شیراز، Pezeshkian1360@gmail.com

چکیده

متدولوژی تحلیل مخاطرات مورد استفاده در این مقاله با اقتباس از مفاهیم دو استاندارد ISA/IEC 62443 و IEC 62351 می باشد. در این متدولوژی ابتدا شبکه و سیستم مورد نظر(پست های فوق توزیع و انتقال) به خوبی شناخته شده و توپولوژی شبکه و دارایی های آن ها مشخص شده است. این گام از پروژه در فاز شناخت امنیت سایبری انجام شده است. در مرحله بعد سیستم مورد نظر، به نواحی مختلف تقسیم‌بندی شده و مجاری و کانال های ارتباطی هر ناحیه مشخص می گردد و برای هر ناحیه و کانال ارتباطی، ارزیابی و تحلیل مخاطرات امنیتی انجام می‌شود.

کلمات کلیدی

امنیت، مخاطرات، ایستگاه، انتقال

۱- مقدمه

تحلیل مخاطرات با اقتباس از مفاهیم مندرج در استاندارد عام صنعتی ISA/IEC 62443 قسمت 2-3-62443 و استاندارد خاص صنعت برق IEC 62351 قسمت 10-62351 انجام شده است. لازم بذکر است که استانداردها بنا بر نقشی که در صنعت دارند از جامعیت بسیاری برخوردار بوده و جزییات سطوح مختلف را در بر می گیرند. در این مقاله سعی شده است با حفظ چارچوب مفاهیم و روش های توصیه شده در استانداردهای مزبور، بنا بر محدوده و نیاز ، از این استانداردها بصورت سفارشی سازی شده استفاده شود[۱].

استاندارد 2-3-62443 به توصیف چگونگی تحلیل و ارزیابی مخاطرات امنیتی سیستم‌های IACS[۱] می پردازد. در این استاندارد متدولوژی کلی تحلیل مخاطرات امنیتی بیان شده و در آن کلیت گام های ارزیابی مخاطرات برای سیستم های IACS تبیین شده است. تحلیل مخاطرات امنیتی در این استاندارد با بخش‌بندی سیستم مورد نظر (SUC) [۲]به نواحی مختلف و مشخص نمودن مجاری و کانال های ارتباطی بین این نواحی شروع می‌شود.

یک ناحیه به گروهی منطقی یا فیزیکی از دارایی‌ها گفته می‌شود که در معیارهایی نظیر موقعیت مکانی و جغرافیایی، وظایف عملکردی و منطقی، عملیات و سطح حساسیت امنیتی، وضعیت مشابه داشته باشند. دارایی‌های موجود در هر ناحیه مشخصه‌های امنیتی مشترکی داشته و به مکانیزم‌های

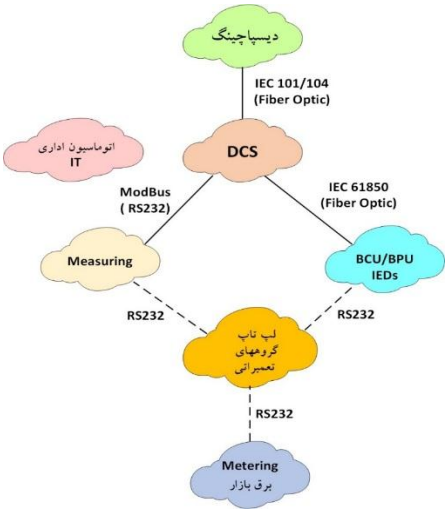
[۱] Industrial Automation and Control System

[۲] System Under Consideration

امنیتی مشـــترکی برای کم کردن ریســـک نیـاز دارند. مجاری به گروهی منطقی از کانال های ارتباطی هر ناحیه گفته می شـــود که نیازمندی های امنیتی یکسانی دارند و دو یا تعداد بیشتری ناحیه را به هم متصل می‌کند. اســـتـانـدارد IEC 62351 متعلق بـه کمیته فنی ۵۷ IEC کارگروه ۱۵ (ISO/IEC TC 57 WG 15) بوده و حوزه آن، امنیـت داده و اطلاعات برای مدیریت سیستم‌های قدرت و اطلاعات مرتبط مبادله شده بین اجزای سیستم‌های قدرت می‌باشد. قسمت دهم استاندارد IEC 62351 راهنمایی کلی در خصـــوص معماری ســـیســـتم های قدرت با تمرکز بر امنیت ارائه می دهد. در بخش 62351-10 این اســـتاندارد، اقدام به معرفی متدولوژی تحلیل مخاطرات امنیتی می کند.

۲- نواحی مختلف پست

بر اساس مفاهیم مندرج در استاندارد ISA/IEC 62443، بمنظور تحلیل مخاطرات امنیتی سیستم صنعتی در حال بررسی(SUC)، ابتدا لازم است سیستم مورد نظر به نواحی(Zone) مختلف تقسیم بندی شده و مجاری(Conduit) و کانالهای ارتباطی بین نواحی مشخص گردد. در این مقاله منظور از SUC، پست انتقال می باشد. یک ناحیه به گروهی منطقی یا فیزیکی از دارایی‌ها گفته می‌شود که در معیارهایی نظیر موقعیت مکانی و جغرافیایی، وظایف عملکردی و منطقی، عملیات و سطح حساسیت امنیتی، وضعیت مشابه داشته باشند. دارایی‌های موجود در هر ناحیه مشخصه‌های امنیتی مشترکی داشته و به مکانیزم های امنیتی مشترکی برای کم کردن ریسک نیاز دارند. مجاری(Conduit) به گروهی منطقی از کانال‌های ارتباطی گفته می‌شود که نیازمندی‌های امنیتی یکسانی دارند و دو یا تعداد بیشتری ناحیه(Zone) را به هم متصل می‌کنند[۲]. شکل (۱) نواحی و مجاری ارتباطی موجود در این پست را نشان می دهد.



شکل(۱) : نواحی و مجاری ارتباطی پست

در جدول (۱) نواحی و مجاری ارتباطی پست مشخص شده است.

جدول(۱) نواحی و مجاری

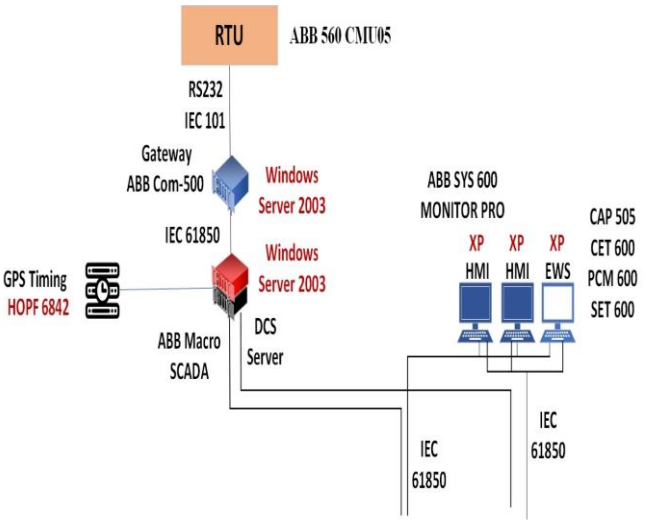
نواحی (Zones)	دیسپاچینگ DCS BCU/BPU Measuring
مجاری (Conduits)	IEC 61850 (Fiber Optic) ModBus (RS232) RS232

۳- تحلیل مخاطرات امنیتی

در این بخش، تحلیـل مخاطرات امنیتی نواحی(Zones) مختلف انجام می شود.

۳-۱- ناحیه DCS

شـکل (۲)، تجهیزات و شـبکه ارتباطی مستقر در ناحیه DCS در ایستگاه مورد مطالعه را نشان می دهد.



شکل(۲) تجهیزات و شبکه ارتباطی ناحیه DCS

در جداول زیر تحلیل مخاطرات امنیتی، کنترل و راهکار بخش های مختلف در این ناحیه آمده است[۳]. که شامل تحلیل مخاطرات امنیتی تجهیز RTU جدول (۲)، تحلیل مخاطرات امنیتی HMI جدول (۳)، تحلیل مخاطرات امنیتی ENG جدول (۴)، تحلیل مخاطرات امنیتی DCS Server جدول (۵)، تحلیل مخاطرات امنیتی DCS Gateway جدول (۶)، تحلیل مخاطرات امنیتی شبکه[۴] DCS جدول (۷). لازم به ذکر است به دلیل عدم وجود پشتیبانی نرم افزار های سیستم اتوماسیون از طرف شرکت ABB ، در این مدل امکان ارتقاء سیستم عامل از ویندوز XP به سیستم عامل بالاتر وجود ندارد، به همین دلیل سعی گردیده مخاطرات بر اساس سیستم عامل های موجود صورت پذیرد.

جدول(۲) تحلیل مخاطرات امنیتی تجهیز RTU

مخاطره	کنترل امنیتی	راهکار
در اختیار گرفتن کنترلRTU و امکان ارسال فرامین غیر مجاز به تجهیزات حفاظتی کنترلی BCU/BPU و خارج شدن پست از شبکه	بکارگیری رمزعبور پیچیده مقاوم سازی RTU	RTU Security Hardening
امکان ارسال فرامین غیر مجاز بالادستی(مرکز دیسپاچینگ) از طریق RTU به تجهیزات حفاظتی کنترلی BCU/BPU	قراردادن سوییچ Remote/Local در حالت Local	
دسترسی افراد غیر مجاز به RTU	بکارگیری رمزعبور پیچیده	
تنظیمات نا امن سیستمی	مقاوم سازی امنیتی	
قطع ارتباط پست با مرکز دیسپاچینگ ملی و محلی	بکارگیری رمزعبور پیچیده مقاوم سازی امنیتی RTU	
عدم اطلاع و آگاهی از رخدادها و عدم وجود امکان فارنزیک	ثبت و جمع آوری و تحلیل رخدادها	
از سرویس خارج شدن RTU	بکارگیری افزونه (Redundancy)	

جدول(۳) تحلیل مخاطرات امنیتی HMI

مخاطره	کنترل امنیتی	راهکار
انتشار بد افزار از طریق فلش و دیگر تجهیزات قابل حمل	تدوین سیاست تجهیزات قابل حمل آنتی ویروس EDP	HMI Security
تنظیمات نا امن سیستمی	مقاوم سازی امنیتی	
افزایش حمله پذیری سیستم در اثر باز بودن پورتها و سرویسهای غیر ضروری	ارتقا و مقاوم سازی امنیتی	
در اختیار گرفتن کنترل HMI و صدور فرامین غیر مجاز برای تجهیزات حفاظتی کنترلی BCU/BPU از طریق DCS Server	مقاوم سازی امنیتی	
نصب غیر مجاز نرم افزارها و دسترسی به تجهیزات حفاظتی کنترلی BCU/BPU	مقاوم سازی امنیتی	

در اختیار گرفتن کنترل HMI و ارتباط مستقیم با سرور از طریق RDP و ایجاد عملیات مخرب	مقاوم سازی امنیتی	
عدم اطلاع و آگاهی از رخدادها و عدم وجود امکان فارنزیک	ثبت و جمع آوری و تحلیل رخدادها	
دان شدن HMI و خارج شدن قابلیت کنترل پست از دست اپراتور	پشتیبان گیری	
دسترسی افراد غیر مجاز به HMI	شناسایی و احرازاصالت کاربران	
انکار پذیری اقدامات انجام شده توسط اپراتور	شناسایی و احرازاصالت کاربران	
ایجاد غیر مجاز اکانت جدید	مدیریت مستمر اکانتها	
استفاده از اکانتهای غیر مجاز نظیر اکانت کارمندان سابق	مدیریت مستمر اکانتها	
امکان بروز حملات دیکشنری	بکارگیری رمزعبور پیچیده	

جدول(۴) تحلیل مخاطرات امنیتی ENG (EWS)

مخاطره	کنترل امنیتی	راهکار
انتشار بد افزار از طریق فلش و دیگر تجهیزات قابل حمل	تدوین سیاست تجهیزات قابل حمل آنتی ویروس EDP	ENG Security
تنظیمات نا امن سیستمی	مقاوم سازی امنیتی	
در اختیار گرفتن کنترل ENG و تغییر تنظیمات یا صدور فرامین غیر مجاز برای تجهیزات حفاظتی کنترلی BCU/BPU	مقاوم سازی	
نصب غیر مجاز نرم افزارها و دسترسی به تجهیزات حفاظتی کنترلی BCU/BPU	مقاوم سازی امنیتی	
در اختیار گرفتن کنترل ENG و ارتباط مستقیم با سرور از طریق RDP و ایجاد عملیات مخرب	مقاوم سازی امنیتی	

عدم اطلاع و آگاهی از رخدادها و عدم وجود امکان فارنزیک	ثبت و جمع آوری و تحلیل رخدادها	
در اختیار گرفتن کنترل ENG و تغییر تنظیمات یا صدور فرامین غیر مجاز برای DCS Server	مقاوم سازی	
در اختیار گرفتن کنترل ENG و تغییر تنظیمات یا صدور فرامین غیر مجاز برای DCS Gateway	مقاوم سازی	
دسترسی افراد غیر مجاز به ENG	شناسایی و احرازاصالت کاربران	
انکار پذیری اقدامات انجام شده	شناسایی و احرازاصالت کاربران	
ایجاد غیر مجاز اکانت جدید	مدیریت مستمر اکانتها	
امکان بروز حملات دیکشنری	بکارگیری رمزعبور پیچیده	
افزایش حمله پذیری سیستم در اثر باز بودن پورتها و سرویسهای غیر ضروری	ارتقا و مقاوم سازی امنیتی	
دان شدن ENG	پشتیبان گیری	

جدول(۵) تحلیل مخاطرات امنیتی DCS Server

مخاطره	کنترل امنیتی	راهکار
در اختیار گرفتن کنترل DCS Server و صدور فرامین غیر مجاز به تجهیزات حفاظتی کنترلی BCU/BPU	مقاوم سازی	DCS Server Security
سرقت اطلاعات از طریق فلش و دیگر تجهیزات قابل حمل	تدوین سیاست تجهیزات قابل حمل Endpoint Protection	
انتقال بد افزار از طریق فلش و دیگر تجهیزات قابل حمل	تدوین سیاست تجهیزات قابل حمل آنتی ویروس Endpoint Protection	
ایجاد خدشه در اطلاعات سیستم	آنتی ویروس لیست سفید بستن پورت ها	

دسترسی غیر مجاز به اطلاعات ذخیره سازی شده	رمزنگاری اطلاعات حساس	
از دست رفتن اطلاعات حساس	پشتیبان گیری فایلها	
تنظیمات نا امن سیستمی	مقاوم سازی امنیتی	
تسخیر سیستم از طریق RDP	مقاوم سازی امنیتی	
افزایش حمله پذیری سیستم در اثر باز بودن پورتها و سرویسهای غیر ضروری	ارتقا و مقاوم سازی امنیتی	
عدم اطلاع و آگاهی از رخدادها و عدم وجود امکان فارنزیک	ثبت و جمع آوری و تحلیل رخدادها	
در اختیار گرفتن کنترل DCS Server و قطع ارتباط با مراکز دیسپاچینگ	مقاوم سازی	
در اختیار گرفتن کنترل DCS Server و از دست دادن دسترسی به آرشیو	مقاوم سازی پشتیبان گیری	
در اختیار گرفتن کنترل DCS Server و از دست رفتن HMI و کارایی اپراتور	دستی یا رله	
در اختیار گرفتن کنترل DCS Server و گمراه کردن اپراتور مرکز دیسپاچینگ، رفتن به حالت سیموله و غیر واقعی نشان دادن وضعیت بریکرها	مقاوم سازی	
امکان بروز حملات دیکشنری	بکارگیری رمزعبور پیچیده	
دان شدن سیستم DCS Server	مقاوم سازی پشتیبان گیری سیستمی	
امکان نصب نرم افزار غیر مجاز	لیست سفید	

جدول(۶) تحلیل مخاطرات امنیتی DCS Gateway

مخاطره	کنترل امنیتی	راهکار
در اختیار گرفتن کنترل DCS Gateway و صدور فرامین غیر مجاز به تجهیزات BCU/BPU	مقاوم سازی امنیتی	DCS Gateway Security
دسترسی افراد غیر مجاز به Gateway	شناسایی و احرازاصالت کاربران	
انتقال بد افزار از طریق فلش و دیگر تجهیزات قابل حمل	تدوین سیاست تجهیزات قابل حمل آنتی ویروس DLP	

عدم اطلاع و آگاهی از رخدادها و عدم وجود امکان فارنزیک	ثبت و جمع آوری و تحلیل رخدادها	
تنظیمات نا امن سیستمی	مقاوم سازی امنیتی	
افزایش حمله پذیری سیستم در اثر باز بودن پورتها و سرویسهای غیر ضروری	ارتقا و مقاوم سازی امنیتی	
در اختیار گرفتن کنترل DCS Gateway و قطع ارتباط با مرکز دیسپاچینگ	مقاوم سازی امنیتی	
دان شدن سیستم	پشتیبان گیری	
در اختیار گرفتن کنترل DCS Gateway و گمراه کردن اپراتور مرکز دیسپاچینگ، رفتن به حالت سیموله و عوضی نشان دادن وضعیت بریکرها	مقاوم سازی امنیتی	
امکان نصب نرم افزار غیر مجاز	لیست سفید	

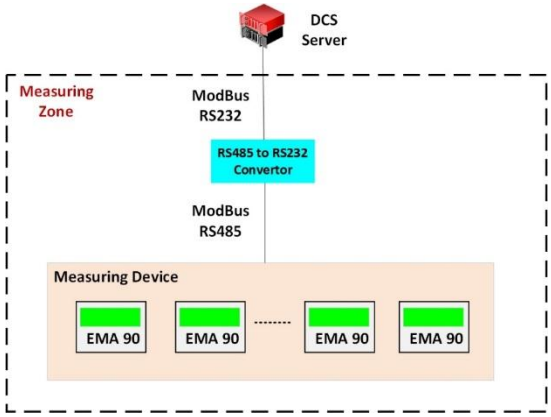
جدول(۷) تحلیل مخاطرات امنیتی شبکه DCS

مخاطره	کنترل امنیتی	راهکار
امکان صدور فرمان اتوماتیک جعلی قطع بریکر و بدنبال آن قطع فیدر و خط انتقال یا فوق توزیع مربوطه و بدنبال آن گسترش حادثه به پستهای همجوار و فروپاشی کل یا بخشی از شبکه	مقاوم سازی تجهیزات شبکه فیلترینگ ترافیک غیر مجاز امن سازی ترافیک MMS فعالسازی رخدادهای سیستمی و تجهیزات شبکه تحلیل رخدادهای تجهیزات و ترافیک شبکه	Industrial Switch Hardening Industrial Firewall MMS Authentication SIEM
عدم اطلاع و آگاهی از رخدادها در شبکه و عدم امکان فارنزیک رخدادها در شبکه	ثبت و جمع آوری و تحلیل رخدادها	فعالسازی رخدادها SIEM
عدم آگاهی به موقع از بروز حملات و در نتیجه عدم بروز عکس العمل به موقع	ثبت و جمع آوری و تحلیل رخدادها	فعالسازی رخدادها سیستمی و شبکه ای SIEM
عدم نظارت مستمر بر وضعیت شبکه و سیستمها و اطلاع یابی دیرهنگام ازحملات	ثبت و جمع آوری و تحلیل رخدادها و پایش مستمر ترافیک	SOC/CERT
خرابکاری روی سرویسهای مبتنی بر زمان و عدم تحلیل زمانی مناسب رخدادها	استفاده از مهر زمانی در رخدادها همزمان سازی تجهیزات	Time Server
انتشار بدافزار در شبکه	تشخیص و مقابله با بد افزار	Anti Virus NGIDS
عدم اطلاع مستمر از رخدادهای شبکه و سیستمها و عدم امکان عملیات تحقیق و بررسی مناسب و جامع	ثبت و جمع آوری و تحلیل رخدادها	فعالسازی رخدادها SIEM
عدم نظارت مستمر بر وضعیت شبکه و سیستمها و اطلاع یابی دیرهنگام ازحملات	ثبت و جمع آوری و تحلیل رخدادها و پایش مستمر ترافیک	SOC/CERT
تنظیمات پیش گزیده و ناامن تجهیزات سوییچنگ	مقاوم سازی امنیتی	Switch Security Hardening
انتشار ترافیک غیر مجاز در شبکه	جداسازی سگمنتهای مختلف شبکه فیلترینگ ترافیک	Network Segmentation Firewall
دسترسی غیر مجاز به سیستمها و تجهیزات سگمنتهای مختلف شبکه	جداسازی سگمنتهای مختلف شبکه فیلترینگ ترافیک	Network Segmentation Firewall
غیرقابل استفاده شدن شبکه بدلیل Storm	جداسازی سگمنتهای مختلف شبکه	Network Segmentation
از دست رفتن ارتباط HMI با DCS Server و DCS Gateway	مقاوم سازی	مقاوم سازی تجهیزات سوییچینگ شبکه
از دست رفتن ارتباط ENG با تجهیزات حفاظتی کنترلی	مقاوم سازی	مقاوم سازی تجهیزات سوییچینگ شبکه
از دست رفتن ارتباط ENG با DCS Server	مقاوم سازی	مقاوم سازی تجهیزات سوییچینگ شبکه

از دست رفتن ارتباط DCS Server با تجهیزات حفاظتی کنترلی	مقاوم سازی	مقاوم سازی تجهیزات سوییچینگ شبکه
از دست رفتن ارتباط DCS Gateway با تجهیزات حفاظتی کنترلی	مقاوم سازی	مقاوم سازی تجهیزات سوییچینگ شبکه
امکان وجود درب پشتی در تجهیزات و بروز حملات شناخته شده یا Zero day	فعالسازی رخدادهای سیستمی و تجهیزات شبکه تحلیل رخدادهای تجهیزات و ترافیک شبکه	SIEM
شنود ترافیک صنعتی	الگوریتم رمزنگاری استاندارد تونلینگ ترافیک	VPN TLS بکارگیری الگوریتم رمزنگاری استاندارد در پروتکل صنعتی

۳-۲- ناحیه Measuring

شکل (۳)، ناحیه Measuring را نشان می دهد.



شکل(۳) ناحیه Measuring

در جـدول (۸) تحلیل مخاطرات امنیتی، کنترل و راهکار بخشـــهای مختلف در این ناحیه آمده است.

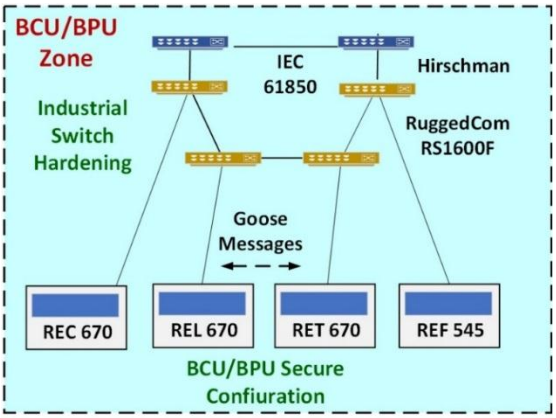
جدول(۸) تحلیل مخاطرات امنیتی Measuring

مخاطره	کنترل امنیتی	راهکار
تغییر پارامترهای اندازه گیری تجهیزات EMA 90 از طریق بدست گرفتن کنترل DCS Server	مقاوم سازی امنیتی پیکربندی امن	مقاوم سازی امنیتی سیستم عامل DCS Server پیکربندی امن DCS Server
تغییر پارامترهای اندازه گیری تجهیزات EMA 90 از طریق بدست گرفتن کنترل DCS Gateway و به اشتباه انداختن دیسپاچینگ	مقاوم سازی امنیتی پیکربندی امن	مقاوم سازی امنیتی سیستم عامل DCS Gateway پیکربندی امن DCS Gateway
انتقال بدافزار از طریق فلش از شبکه IT به OT بکارگیری فلش جهت انتقال اطلاعات روی سیستم اتوماسیون اداری	تعریف فلشهای تراست	Endpoint Protection
دسترسی غیر مجاز از طریق بکارگیری کلمات عبور پیش فرض در تجهیزات EMA 90	مدیریت کلمات عبور	مدیریت کلمات عبور
امکان قرائت پارامترهای EMA از طریق دسترسی فیزیکی به Operation Panel و تغییر تنظیمات	کنترل دسترسی فیزیکی احراز اصالت کاربر	کنترل دسترسی فیزیکی احراز اصالت کاربر

۳-۳- ناحیه BCU/BPU

در این ناحیه انواع تجهیزات حفاظتی کنترلی پست مستقر بوده و از طریق شبکه ارتباطی مبتنی بر IEC 61850 با هم در ارتباط هستند[۵] ، [۶].

شکل (4)، ناحیه BCU/BPU را نشان می دهد.



شکل(4) ناحیه BCU/BPU

در جـداول زیر تحلیل مخاطرات امنیتی، کنترل و راهکار بخشـــهای مختلف در این ناحیه آمده است.

جدول(۹) تحلیل مخاطرات امنیتی شبکه ارتباطی تجهیزات BCU/BPU

مخاطره	کنترل امنیتی	راهکار
ایجاد اختلال در ترافیک ارتباطی تجهیزات BCU/BPU	بکارگیری افزونگی برای تجهیزات مقاوم سازی تجهیزات شبکه فیلترینگ ترافیک غیر مجاز	Redundancy Industrial Firewall Industrial Switch Hardening
عدم آگاهی به موقع از بروز حملات و در نتیجه عدم بروز عکس العمل به موقع	ثبت و جمع آوری و تحلیل رخدادها	فعالسازی رخدادها سیستمی و شبکه ای SIEM
عدم نظارت مستمر بر وضعیت شبکه و سیستمها و اطلاع یابی دیرهنگام ازحملات	ثبت و جمع آوری و تحلیل رخدادها و پایش مستمر ترافیک	SOC/CERT
عدم اطلاع و آگاهی از رخدادها در شبکه و عدم امکان فارنزیک رخدادها در شبکه	ثبت و جمع آوری و تحلیل رخدادها	فعالسازی رخدادها SIEM
خرابکاری روی سرویسهای مبتنی بر زمان و عدم تحلیل زمانی مناسب رخدادها	استفاده از مهر زمانی در رخدادها همزمان سازی تجهیزات	Time Server
ایجاد اختلال و قطعی در شبکه ارتباطی DCS و رله ها و عدم امکان صدور فرمان اتوماتیک به رله ها و تبدیل عملکرد پست به Conventional	بکارگیری افزونگی برای تجهیزات مقاوم سازی تجهیزات شبکه فیلترینگ ترافیک غیر مجاز	Redundancy Industrial Firewall Industrial Switch Hardening
ارسال ترافیک جعلی بین تجهیزات BCU/BPU	مقاوم سازی تجهیزات شبکه فیلترینگ ترافیک غیر مجاز احراز اصالت پیامهای Goose	Industrial Firewall Industrial Switch Hardening Goose Authentication
امکان وجود درب پشتی در تجهیزات و بروز حملات شناخته شده یا Zero day	فعالسازی رخدادهای سیستمی و تجهیزات شبکه تحلیل رخدادهای تجهیزات و ترافیک شبکه	SIEM
انتشار ترافیک غیر مجاز در شبکه	جداسازی سگمنتهای مختلف شبکه فیلترینگ ترافیک	Network Segmentation Firewall

جدول(۱۰) تحلیل مخاطرات امنیتی تجهیزات حفاظتی کنترلی BCU/BPU

مخاطره	کنترل امنیتی	راهکار
دسترسی افراد غیر مجاز به تجهیزات BCU/BPU از طریق کلمات عبور ضعیف یا پیش فرض و تغییر تنظیمات و صدور فرامین غیر مجاز	مدیریت کلمات عبور	BCU/BPU Hardening
آسیب پذیری بدلیل عدم بروزرسانی ثابت افزار	بروزرسانی ثابت افزار از منابع مطمئن	BCU/BPU Hardening بروزرسانی ثابت افزار از منابع مطمئن
انتقال بد افزار از طریق ارتباط لپ تاپ با تجهیزات BCU/BPU	امن سازی لپ تاپ	Laptop Hardening
امکان قرائت پارامترهای BCU/BPU از طریق دسترسی فیزیکی به Operation Panel	کنترل دسترسی فیزیکی مدیریت کلمه عبور	کنترل دسترسی فیزیکی BCU/BPU Hardening
امکان صدور فرمان به BCU/BPU از طریق دسترسی فیزیکی به Operation Panel و داشتن کلمات عبور IED	کنترل دسترسی فیزیکی مدیریت کلمه عبور	کنترل دسترسی فیزیکی BCU/BPU Hardening
ایجاد اختلال در فرایندهای کنترلی یا حفاظتی BCU/BPU بدلیل در اختیار نداشتن کلمه عبور تجهیز بمنظور تغییر پیکربندی مورد نیاز	مدیریت کلمات عبور	جایگزینی تجهیز

۴- نتیجه گیری

پس از تحلیل مخاطرات با استفاده از ابزار پویش آسیب پذیری Nessus اقدام به پویش رخنه ها و آسیب پذیریهای امنیتی سیستم DCS شده است[۷]. از آنجایی که استفاده از ابزارهای پویش آسیب پذیری خودکار در محیط عملیاتی، تاثیرات غیرقابل پیش بینی بر روی عملکرد تجهیزات صنعتی خواهد داشت، عملیات پویش آسیب پذیری در شرایط آزمایشگاهی و بصورت کاملا ایزوله از محیط عملیاتی انجام شد. در این پویش پورت های باز سیستم مهندسی، سرور، Gateway و WSها از نظر سطوح آسیب پذیری مورد بررسی قرار گرفت (آسیب پذیری بحرانی، آسیب پذیری مهم و آسیب پذیری متوسط). همچنین محل های نصب سنسورها جهت سیستم SOC مشخص گردید[۸].

مراجع

[1] E. Ciapessoni, D. Cirio, A. Pitto, “Contingency screening starting from probabilistic models of hazards and component vulnerabilities ,” 19th Power Systems Computation Conference - Papers submission and review system, June 2016, PP. 1-8.
[2] S. McClure, J. Scam bray, and G. Kurtz, “Hacking Exposed: Network Security Secrets and Solutions”, 4th ed. Emeryville, CA: McGraw-Hill, 2003.
[3] C.-W. Ten, C.-C. Liu, and G. Manimaran, “Vulnerability Assessment of Cyber security for SCADA Systems,” IEEE Trans. Power Syst., Vol.23, No. 4, Nov. 2008, PP. 1836–1846.
[4] N. Liu, J. Zhang, H. Zhang, and W. Liu, “Security Assessment for Communication Networks of Power Control Systems Using Attack Graph and MCDM,” IEEE Trans. Power Deliv., Vol. 25, No. 3, Jul. 2010, PP.1492–1500.
[5] L. Hossenlopp, “Engineering perspectives on IEC 61850,” IEEE Power and Energy Magazine, Vol. 5, No. 3, May 2007, PP. 45-50.
[6] IEC 61850-6 standard, Configuration description language for communication in electrical substations related to IEDs, 1st ed. International Electrotechnical Commission, Mar. 2004.
[7] C.-C. Liu, A. Stefanov, J. Hong, and P. Panciatici, “Intruders in the Grid,” IEEE Power Energy Mag., Vol. 10, No. 1, Jan. 2012, PP. 58–66.
[8] J. Yue, and K. Zhang, “vulnerability Threat Assessment based on AHP and Fuzzy Comprehensive Evaluation,” Computional Intelligent and Design(ISCID), 2014 Seventh Internation Symposiumon,Vol.2, Dec.2014, PP.513-516.