

۱۷/۱۰/۱۳۹۱

بسم الله الرحمن الرحيم

مرجع کاربردی

امنیت سایبری سامانه‌های کنترل صنعتی

(Industrial Control Systems Cyber Security)

نویسنده:

مهندس م. عبدالعزیز

- سرشناسه: عبدالتاج‌دینی، محمد، ۱۳۶۶
- عنوان و نام پدیدآور: مرجع کاربردی امنیت سایبری سامانه‌های کنترل صنعتی - security Industrial control systems cyber
- نویسنده: محمد عبدالتاج‌دینی.
- مشخصات نشر: تهران: انتشارات ایده نگار، ۱۳۹۷.
- مشخصات ظاهری: ۴۷۰ ص: مصور، جدول، نمودار.
- ISBN: 978-600-8304-38-8

- وضعیت فهرست نویسی: فیا
- موضوع: کنترل فرایندها - پیش‌بینی‌های ایمنی
- موضوع: Process control - Security measures
- موضوع: کامپیوترها - ایمنی اطلاعات
- موضوع: Computer security
- موضوع: سیستم‌های کنترل تطبیقی
- موضوع: Adaptive control systems
- موضوع: سامانه‌های کنترل بازخورد - پیش‌بینی‌های ایمنی
- موضوع: Feedback control system - Security measures
- رده بندی کنگره: ۱۳۹۶ ۴۲۵/۸/۵۱۸۶
- رده بندی دیویی: ۶۷۰/۴۲۷۵
- شماره کتابشناسی ملی: ۵۱۱۱۰۷۶



..... نشر ایده نگار www.iNegar.ir

مرجع کاربردی

امنیت سایبری سامانه‌های کنترل صنعتی

| نویسنده: مهندس محمد عبدالتاج‌دینی |

| ناظر چاپ: مهندس هادی غریبی |

| ویراستار: مهندس هادی غریبی |

| صفحه‌آرا و طراح جلد: مهندس معصومه باباپور |

| نوبت چاپ: اول، ۱۳۹۷ | شمارگان: ۱۰۰۰ |

| شابک: ۹۷۸-۶۰۰-۸۳۰۴-۳۸-۸ |

کلیه حقوق قانونی این اثر متعلق به نشر ایده نگار می‌باشد.

تکثیر تمام یا قسمتی از این اثر به هر شکل ممنوع است.

متخلفان به موجب قانون حمایت از مؤلفان، مصنفان و هنرمندان تحت پیگرد قانونی قرار می‌گیرند.
نشانی مرکز بخش: تهران، میدان انقلاب، کوچه شهید رشتچی، پلاک ۱۳، طبقه دوم، واحد ۴

مقدمه ناشر / ۱۵

دیباجه نویسنده / ۱۷



درباره این کتاب (About this Book)

درباری این کتاب / ۲



فصل اول

ساختار و معماری سامانه‌های کنترل صنعتی

ساختار و معماری سامانه‌های کنترل / ۲۶

۱-۱. سامانه کنترل زیمنس / ۳۰

۱-۱-۱. کنترل‌کننده‌های معمولی S7-400 / ۳۵

۱-۱-۲. کنترل‌کننده‌های S7-400 H با قابلیت افزودنی / ۳۶

۱-۱-۳. کنترل‌کننده‌های S7-400 FH با قابلیت استفاده در محیط‌های خطرناک / ۳۶

۱-۴. تجهیزات سخت‌افزاری مورد استفاده در PCS7 / ۳۷

۱-۵. سامانه مانیتورینگ (HMI) در PCS7 زیمنس / ۴۸

۲-۱. سامانه کنترل یو‌کو‌گاوا / ۴۹

۲-۱-۱. Field Control Station / ۵۲

۲-۲. Human Interface Station / ۵۶

۲-۳-۱. شبکه ارتباطی V-NET / ۵۹

۳-۱. سامانه کنترل ABB / ۶۱

۳-۱-۱. سامانه کنترل ABB مدل AC 800F / ۶۴



فصل دوم

امنیت در سازمان‌ها و زیرساخت‌های صنعتی

- ۱-۲. امنیت در زیرساخت‌های صنعتی / ۸۲
- ۱-۱-۲. ریسک، تهدید و آسیب‌پذیری / ۸۳
- ۲-۱-۲. ریسک / ۸۴
- ۳-۱-۲. تهدید / ۸۵
- ۴-۱-۲. آسیب‌پذیری / ۸۵
- ۲-۱. اصول مدیریت و کاهش ریسک / ۸۶
- ۱-۲-۲. فرآیند مدیریت ریسک / ۸۶
- ۲-۲-۲. فرایند کاهش ریسک / ۸۹
- ۳-۲. امنیت در سامانه‌های کنترل صنعتی / ۹۰
- ۱-۳-۲. مقایسه سامانه‌های کنترل و صنعتی / ۹۱
- ۱-۱-۳-۲. تمرکز بر ساختار امنیت / ۹۱
- ۲-۱-۳-۲. آزمایشات سامانه‌های حوزه IT صنعتی / ۹۳
- ۳-۱-۳-۲. محدودیت‌های منابع / ۹۳
- ۴-۱-۳-۲. شبکه و بسترهای ارتباطی / ۹۴
- ۵-۱-۳-۲. اعمال تغییرات در سامانه / ۹۴
- ۶-۱-۳-۲. خدمات و پشتیبانی / ۹۵
- ۷-۱-۳-۲. طول عمر تجهیزات / ۹۵
- ۸-۱-۳-۲. الزامات بهره‌برداری / ۹۶
- ۹-۱-۳-۲. ری‌استارت کردن سامانه / ۹۶
- ۱۰-۱-۳-۲. میزان تحمل خطا / ۹۶
- ۱۱-۱-۳-۲. بخش حفاظت / ۹۶
- ۱۲-۱-۳-۲. راهکارهای امنیتی / ۹۷
- ۱۳-۱-۳-۲. پاسخگویی در زمان بحران / ۹۷
- ۱۴-۱-۳-۲. کنترل دسترسی / ۹۷
- ۱۵-۱-۳-۲. سیستم‌عامل / ۹۸
- ۴-۲. امنیت از دیدگاه فیزیکی / ۹۸

- ۴-۱. کنترل فیزیکی ورود و خروج / ۹۸
- ۴-۲. دفاتر، اتاق‌ها و تاسیسات امن / ۹۹
- ۴-۳. جداسازی مناطق ارسال و دریافت / ۱۰۰
- ۵-۲. امنیت از دیدگاه مدیریتی / ۱۰۲
- ۶-۲. امنیت از دیدگاه فنی / ۱۰۶
- ۷-۲. بخش‌های امنیت سایبری سامانه‌های کنترل صنعتی / ۱۰۹
- ۷-۲-۱. امنیت فیزیکی شبکه / ۱۱۰
- ۷-۲-۲. امنیت زیرساخت شبکه / ۱۱۰
- ۷-۲-۳. امنیت پروتکل / ۱۱۱
- ۷-۲-۴. امنیت سیستم‌عامل و نرم‌افزارها / ۱۱۱
- ۷-۲-۵. آه‌زش کاران و مدیران شبکه / ۱۱۲
- ۷-۲-۶. مانیتورینگ، میزور و مدیریت متمرکز / ۱۱۲
- ۷-۲-۷. پشتیبان‌گیری / ۱۱۲
- ۷-۲-۸. مستندسازی / تدوین خط‌مشی‌ها و دستورالعمل‌های امنیتی / ۱۱۳
- ۷-۲-۹. اشتباهات متداول مدیران امنیتی / ۱۱۳
- ۷-۲-۱۰. اشتباهات متداول مدیران شبکه / ۱۱۳
- ۷-۲-۱۱. اشتباهات متداول کاربران معمول / ۱۱۴
- ۸-۲. مباحث فنی مهم در سامانه‌های کنترل صنعتی / ۱۱۴
- ۸-۲-۱. توپولوژی، معماری و نحوه طراحی و پیاده‌سازی سامانه‌های کنترل صنعتی / ۱۱۵
- ۸-۲-۲. چگونگی و نحوه تهیه نسخه پشتیبان، نگهداری و همچنین برگرداندن آن / ۱۱۷
- ۸-۲-۳. تنظیمات و پیکربندی سامانه کنترل و تجهیزات امنیتی / ۱۲۰
- ۸-۲-۴. پیکربندی و تنظیمات امنیتی مربوط به تجهیزات مورد استفاده در شبکه‌های صنعتی (Switch, Router) / ۱۳۳
- ۸-۲-۵. سیستم‌عامل و نرم‌افزارهای صنعتی و غیرصنعتی مورد استفاده / ۱۳۷
- ۸-۲-۵-۱. نوع سیستم‌عامل / ۱۳۷
- ۸-۲-۵-۲. نسخه‌های مختلف نرم‌افزارهای کنترل صنعتی و اسکادا / ۱۳۹
- ۸-۲-۵-۳. به‌روز رسانی سیستم‌عامل‌ها و نرم‌افزارها / ۱۴۰
- ۸-۲-۵-۴. سیستم‌عامل و نرم‌افزارهای کرک شده و غیر اصلی / ۱۴۲
- ۸-۲-۵-۵. نرم‌افزارهای جانبی و متفرقه / ۱۴۳
- ۸-۲-۵-۶. پالیسی‌ها و تنظیمات امنیتی در سیستم‌عامل / ۱۴۳
- ۸-۲-۶. نوع پروتکل‌های صنعتی و پیکربندی آنها / ۱۴۴

- ۷-۸-۲. چگونگی و نحوه امن‌سازی ارتباطات شبکه‌ای و مخابراتی مجتمع صنعتی / ۱۴۴
 ۸-۸-۲. سرویس‌های ارائه شده و در حال اجرا / ۱۴۵
 ۹-۸-۲. سخت‌افزارها و نرم‌افزارهای امنیتی و نحوه پیکربندی آنها / ۱۴۷
 ۱۰-۸-۲. سامانه‌های ESD و F&G و ارتباط آنها با سامانه کنترل اصلی (DCS) / ۱۴۸
 ۱۱-۸-۲. تجهیزات سطح فیلد و نحوه برقراری ارتباط آنها با لایه کنترل / ۱۵۳

۹-۲. دفاع در عمق / ۱۵۶

۱-۹-۲. معماری دفاع در عمق سامانه‌های کنترل صنعتی / ۱۵۸

۱-۱-۹-۲. معماری دفاع در عمق شرکت یو‌کوگاوا / ۱۵۸

۲-۱-۹-۲. معماری دفاع در عمق شرکت امرسون / ۱۶۰

۱-۱-۹-۲. معماری دفاع در عمق شرکت زیمنس / ۱۶۲

۱-۱-۹-۲. جمع‌بندی / ۱۶۵



فصل سوم

تهدیدات و آسیب‌پذیری‌های سامانه‌های کنترل صنعتی

تهدیدات و آسیب‌پذیری‌های سامانه‌های کنترل صنعتی / ۱۷۰

۱-۳. تهدیدات / ۱۷۱

۱-۱-۳. مهاجمین سایبری / ۱۷۱

۲-۱-۳. سامانه‌های کنترل صنعتی مدرن / ۱۷۳

۳-۱-۳. استفاده از تجهیزات و سامانه‌های کنترل صنعتی / ۱۷۳

۴-۱-۳. پیمانکاران / ۱۷۴

۵-۱-۳. عدم وجود تنوع در سامانه‌های کنترل صنعتی / ۱۷۵

۶-۱-۳. بات‌نت‌ها / ۱۷۵

۷-۱-۳. کدهای مخرب و بدافزارهای صنعتی / ۱۷۶

۸-۱-۳. استفاده از سرویس‌ها و خدمات شرکت‌های خارجی / ۱۷۶

۹-۱-۳. پرسنل داخلی / ۱۷۶

۲-۳. آسیب‌پذیری‌ها / ۱۷۷

۱-۲-۳. آسیب‌پذیری‌های سیستمی / ۱۷۸

۱-۲-۳. کنترل‌کننده‌های صنعتی / ۱۷۸

۱- آسیب‌پذیری ذخیره‌سازی ناامن و ضعیف HTTPS CA Certificate / ۱۸۰

۲- آسیب‌پذیری احراز هویت ضعیف و نامناسب / ۱۸۱

- ۳- آسیب‌پذیری سرریز بافر / ۱۸۲
- ۴- آسیب‌پذیری منع سرویس / ۱۸۳
- ۵- آسیب‌پذیری سرریز بافر نوع Heap-Based & Stack-Based / ۱۸۴
- ۳-۲-۱- سیستم‌عامل و نرم‌افزارهای کاربردی / ۱۸۵
- ۱- آسیب‌پذیری در نرم‌افزار WinCC زیمنس / ۱۸۵
- ۲- آسیب‌پذیری در نرم‌افزارهای اسکادا اشنایدرالکترونیک / ۱۸۶
- ۳- آسیب‌پذیری سرریز بافر در وب‌سرور نرم‌افزار VIJE شرکت اشنایدرالکترونیک / ۱۸۷
- ۴- آسیب‌پذیری احراز هویت ضعیف در نرم‌افزار EXAOPC یوگواوا / ۱۸۸
- ۲-۳- شبکه و بسترهای ارتباطی / ۱۸۸
- ۱- آسیب‌پذیری در سوئیچ مربوط به شبکه VNET/IP از محصولات یوگواوا / ۱۸۹
- ۲- آسیب‌پذیری کنترل دسترسی ضعیف در کارت‌های شبکه CP1604، CP1616 شرکت زیمنس / ۱۹۰
- ۳-۲-۲- آسیب‌پذیری‌های غیر سیستمی / ۱۹۱
- ۳-۲-۲-۱- مستقل نبودن ایستگاه‌های پندسی از ایستگاه‌های اپراتوری در اتاق کنترل / ۱۹۲
- ۳-۲-۲-۲- عدم وجود یک روش صحیح پشتیبان‌گیری از سامانه و برگرداندن آن / ۱۹۲
- ۳-۲-۲-۳- عدم تعریف نام کاربری و کلمه عبور / ۱۹۲
- برای اپراتورها و مهندسين کنترل و اراد دقیق / ۱۹۳
- ۳-۲-۲-۴- عدم رعایت مسائل امنیتی توسعه پرسنل / ۱۹۵
- ۳-۲-۲-۵- کمبود سطح دانش فنی و امنیتی پرسنل / ۱۹۶
- ۳-۲-۲-۶- مناقصه‌ها و مزایده‌ها / ۱۹۵
- ۳-۳- مراجع و سایت‌های معرفی آسیب‌پذیری‌های سیستم‌های راه‌ها - کنترل صنعتی / ۱۹۶
- ۳-۳-۱- وبسایت ICS-CERT.US-CERT.GOV / ۱۹۸
- ۳-۳-۲- وبسایت NVD / ۲۰۱
- ۳-۳-۳- وبسایت CVE / ۲۰۴
- ۳-۳-۴- وبسایت CVE Details / ۲۰۵
- ۳-۳-۵- وبسایت Exploit Database / ۲۰۶
- ۳-۳-۶- وبسایت ASIS / ۲۰۹
- جمع‌بندی / ۲۱۰



فصل چهارم

حملات سایبری در سامانه‌های کنترل صنعتی

مقدمه / ۲۱۴

حملات سایبری رایج در دنیای امنیت / ۲۱۵

۱-۴. انکار سرویس (Denial Of Service) / ۲۱۵

۲-۴. تزریق دستورات SQL (SQL Injection) / ۲۱۹

۳-۴. جعل کردن / ۲۲۱

۳-۴. جعل ایمیل / ۲۲۱

۲-۳-۴. پروتکل‌های TCP/IP و جعل کردن / ۲۲۲

۳-۳-۴. جعل اسرک فایل / ۲۲۳

۴-۳-۴. جعل ایمیل صوتی / ۲۲۳

۴-۴. مردی در میان / ۲۲۴

۵-۴. بازیخش یا تکرار / ۲۲۶

۶-۴. بدافزارها یا کدهای مخرب / ۲۲۷

۱-۶-۴. بدافزارهایی که تکثیر می‌شوند / ۲۲۷

۲-۶-۴. بدافزارهایی که مخفی می‌شوند / ۲۲۹

تروجان / ۲۲۹

RootKit / ۲۳۰

Logic Bomb و Backdoor / ۲۳۰

۳-۶-۴. بدافزارهایی که برای سازنده خود سود دارند / ۲۳۱

Spyware یا جاسوس افزار / ۲۳۱

Adware یا تبلیغات افزار / ۲۳۱

Keylogger / ۲۳۲

۷-۴. DEFACE کردن وبسایت / ۲۳۲

۸-۴. مهندسی اجتماعی / ۲۳۲

۱-۸-۴. انواع حمله‌های مهندسی اجتماعی / ۲۳۴

مهندسی اجتماعی مبتنی بر انسان / ۲۳۴

مهندسی اجتماعی مبتنی بر کامپیوتر / ۲۳۵

اقدام‌های متقابل در برابر مهندسی اجتماعی / ۲۳۸

حملات و راه‌های نفوذ به سامانه‌های کنترل صنعتی و اسکادا / ۲۴۰

- ۹-۴. شنود و کپی برداری از اطلاعات تبادل / ۲۴۰
- ۹-۴.۱. شنود اطلاعات و داده‌های تبادل در اتاق کنترل / ۲۴۰
- ۹-۴.۲. شنود اطلاعات و داده‌های تبادل بین اتاق کنترل و بخش اداری / ۲۴۳
- ۹-۴.۳. از کار انداختن وسایل و تجهیزات مسیرهای ارتباطی اسکادا / ۲۴۹
- ۹-۴.۴. نفوذ به بخش‌های مختلف یک نیروگاه و پست انتقال برق / ۲۵۰
- ۹-۴.۵. حمله سایبری بر روی تجهیزات ابزار دقیق مانند ترانسمیترها، ولوها / ۲۵۷
- ۹-۴.۶. حمله سایبری در سامانه کنترل DCS از طریق سامانه ENG / ۲۶۲
- ۹-۴.۷. حمله سایبری از طریق آلوده شدن DCS توسط بدافزارهای صنعتی / ۲۶۳
- ۹-۱. به سرقت رفتن اطلاعات مهم صنعتی و سازمانی در هنگام جابجایی آنها از یک مکان به مکان دیگر / ۲۶۹
- ۹-۴.۹. رفتن اطلاعات کاربری و کلمه عبور مهندسين سامانه‌های کنترل صنعتی / ۲۷۰
- ۹-۴.۱۰. حمله سایبری توسط KEYLOGGER در سامانه‌های کنترل صنعتی و اسکادا / ۲۷۱
- ۹-۴.۱۱. کلمه عبور پیش فرض تجهیزات و نرم‌افزارهای مورد استفاده / ۲۷۵
- ۹-۴.۱۲. فعال نمودن یک برنامه مخفی در یک زمان مشخص / ۲۷۵
- ۹-۴.۱۳. مهندسی اجتماعی حمله به زیرساخت‌های صنعتی از طریق آن / ۲۷۶
- ۴-۱۰. جمع بندی / ۲۷۷

۱-۵. مراکز و سازمان‌های استاندارد معتبر جهانی / ۲۸۲

- ۱-۱-۵. استاندارد NERC / ۲۸۴
- ۲-۱-۵. استاندارد NRC / ۲۸۴
- ۱-۲-۱-۵. NRC TITLE 10 CFR 73.54 / ۲۸۵
- ۲-۲-۱-۵. NRC RG 5.71 / ۲۸۵
- ۳-۱-۵. استاندارد DHS / ۲۸۵
- ۴-۱-۵. استاندارد ISA / ۲۸۶
- ۵-۱-۵. استاندارد ISO و IEC / ۲۸۷
- ۶-۱-۵. استاندارد NIST / ۲۸۷
- ۱-۶-۱-۵. دیواره آتش / ۲۹۰
- ۱-۶-۲. جدا نمودن شبکه صنعتی و غیرصنعتی از لحاظ منطقی / ۲۹۴

- ۱-۲-۶-۱-۵. معماری امنیتی با استفاده از یک دیواره آتش / ۲۹۵
- ۱-۲-۶-۱-۵. معماری امنیتی با استفاده از یک دیواره آتش و یک مسیر یاب / ۲۹۷
- ۱-۲-۶-۱-۵. معماری امنیتی با استفاده از یک دیواره آتش با سه کارت شبکه / ۲۹۸
- ۱-۲-۶-۱-۵. معماری امنیتی با استفاده از دو دیواره آتش / ۳۰۱
- ۱-۲-۶-۳. معماری دفاع در عمق / ۳۰۲
- ۱-۲-۶-۴. سیاست‌های کلی برای دیواره آتش مورد استفاده در شبکه‌های صنعتی / ۳۰۲
- ۱-۲-۶-۵. تنظیم و پیکربندی دیواره آتش برای سرویس‌ها و پروتکل‌های خاص / ۳۰۵
- ۱-۲-۶-۵. سرویس DNS / ۳۰۶
- ۱-۲-۵-۲. پروتکل HTTP / ۳۰۶
- ۱-۲-۶-۱. پروتکل‌های FTP و TFTP / ۳۰۷
- ۱-۲-۵-۴. Telnet / ۳۰۸
- ۱-۲-۵-۵. IMTP / ۳۰۹
- ۱-۲-۵-۶. SMTP / ۳۱۰
- ۱-۲-۵-۷. LCOM / ۳۱۲
- ۱-۲-۵-۸. پروتکل‌های مورد استفاده در شبکه‌های صنعتی / ۳۱۲
- ۱-۲-۵-۹. NAT / ۳۱۳
- ۱-۲-۶-۶. ضعف‌های دیگر معماری شبکه‌های صنعتی با وجود دیواره آتش / ۳۱۳
- ۱-۲-۶-۱. سرورها و منابع مشترک بین شبکه‌های صنعتی و IT / ۳۱۳
- ۱-۲-۶-۲. دسترسی از راه دور به سامانه کنترل صنعتی / ۳۱۴
- ۱-۲-۶-۳. Single Point of Failure / ۳۱۵
- ۱-۲-۶-۴. افزونگی و تحمل خطا / ۳۱۶
- ۱-۲-۶-۷. حمله سایبری MITM / ۳۱۶
- ۱-۲-۶-۱. محدود کردن آدرس MAC / ۳۱۷
- ۱-۲-۶-۲. جداول استاتیک / ۳۱۷
- ۱-۲-۶-۳. رمزنگاری / ۳۱۸
- ۱-۲-۶-۴. نظارت بر آلوده نمودن جداول ARP / ۳۱۸
- ۱-۲-۷-۷. استاندارد NERC / ۳۱۸
- ۱-۲-۸-۸. استاندارد ISA / ۳۲۳
- ۱-۲-۹-۹. سری استانداردهای ISA99 / ۳۲۴
- ۱-۲-۹-۱. تکنولوژی‌های احراز هویت و مجوز / ۳۳۵
- ۱-۲-۹-۲. کنترل دسترسی نقش‌محور (RBAC) / ۳۳۷

- ۳-۹-۱-۵. استفاده از رمزهای عبور / ۳۳۸
- ۵-۹-۱-۵. فیلترینگ/مسدودکردن/کنترل دسترسی / ۳۴۱
- ۶-۹-۱-۵. دیواره‌های آتش شبکه در استاندارد ISA99 / ۳۴۲
- ۷-۹-۱-۵. شبکه‌های محلی مجازی (VLAN) از دیدگاه استاندارد ISA99 / ۳۴۸
- ۸-۹-۱-۵. رمزنگاری و رمزگشایی از دیدگاه استاندارد ISA99 / ۳۴۹
- ۹-۹-۱-۵. شبکه‌های خصوصی مجازی (VPN) / ۳۵۲
- ۱۰-۹-۱-۵. سیستم‌های تشخیص نفوذ / ۳۶۰
- ۱۱-۹-۱-۵. پوششگرهای آسیب پذیری / ۳۶۳
- ۱۲-۱-۵. نرم‌افزار سامانه‌های کنترل صنعتی / ۳۶۵
- ۱۳-۹-۱-۵. ل‌های امنیت فیزیکی / ۳۶۷
- ۱۴-۹-۱-۵. امنیت کارکنان / ۳۶۹
- جمع‌بندی / ۳۷۰

- ۱-۶. محصولات امنیت سایبری در سامانه‌های کنترل صنعتی / ۳۷۶
- ۱-۱-۶. شرکت SIEMENS / ۳۷۶
- ۱-۱-۶. حفاظت بخش‌های مختلف سامانه کنترل صنعتی توسط SCALANCE M / ۳۸۶
- ۲-۶. شرکت ABB / ۳۹۳
- ۳-۶. شرکت YOKOGAWA / ۴۱۶
- ۴-۶. شرکت SCHNEIDER ELECTRIC / ۴۲۹
- ۴-۶. دیواره آتش صنعتی اشتایدرالکترونیک / ۴۳۷
- ۵-۶. شرکت CISCO / ۴۳۹
- ۶-۶. شرکت TOFINO / ۴۴۵
- ۷-۶. شرکت EMERSON / ۴۵۰
- ۸-۶. شرکت ALLEN BRADLEY / ۴۵۶
- ۹-۶. شرکت MOXA / ۴۵۷
- ۱۰-۶. شرکت PHOENIX / ۴۵۸
- جمع‌بندی / ۴۶۰



www.ketab.ir

دیاچه نویسنده

امروزه با حضور تجهیزات و سامانه‌های کنترلی مبتنی بر کامپیوتر^۱ در صنعت، امکان کنترل دقیق‌تری در فرآیندهای صنعتی بوجود آمده است و بسیاری از صنایع بزرگ و کوچک، با تغییر سامانه‌های کنترل قدیمی، به PLC^۲ ها و سامانه‌های DCS^۳ و SCADA^۴ مجهز شده‌اند؛ از طرفی هم‌اکنون با توسعه شبکه‌های کامپیوتری، تجهیزات و سامانه‌های تولید در جهان به سرعت در حال تحول بوده و بسیاری از فرآیندهای صنعتی توسط این سامانه‌ها که دارای مزایای بسیار زیادی نسبت به سایر روش‌ها هستند کنترل می‌شوند. PLC ها، سامانه‌های DCS و SCADA به‌طور گسترده جهت کنترل و نظارت فرآیندهای صنعتی از جمله نفت، گاز، پتروشیمی، برق، هسته-ای و دیگر صنایع بزرگ و کوچک استفاده قرار می‌گیرند. پیشرفت‌های روزافزون در سامانه‌های کنترل صنعتی و تجهیزات مورد استفاده در آنها نه تنها باعث افزایش کارایی و بهبود عملکرد سامانه‌ها و فرآیند شده، بلکه کنترل بسیاری از فرآیندهای ناممکن و یا پیچیده را تسهیل بخشیده و امکان کنترل را در نلارت از راه دور را فراهم ساخته است. امروزه علی‌رغم پیشرفت‌های بسیار زیادی که در ساختار و عملکرد سامانه‌های کنترل صنعتی وجود داشته، این سامانه‌ها از دیدگاه سایبری دارای ضعف‌های بسیار زیادی بوده و همین امر باعث شده که مورد تهدید و حملات سایبری قرار بگیرند. ضعف‌ها و آسیب‌پذیری‌های موجود در بخش‌های مختلف سامانه‌های کنترل صنعتی و اسکادا این امکان را برای مهاجمین سایبری فراهم

^۱ منظور کنترل‌کننده‌های صنعتی می‌باشند که دارای ساختاری شبیه به کامپیوتر هستند.

^۲ Programmable Logic Controller

^۳ Distributed Control Systems

^۴ Supervisory Control And Data Acquisition

ساخته تا حمله به زیرساخت‌های حیاتی کشورها، آسیب‌رساندن و یا ایجاد اختلال در فرآیند کاری آن‌ها را جز اهداف و برنامه‌های خود قرار دهند. از آنجا که بروز هرگونه نارسایی در سامانه‌های کنترل صنعتی و اسکادا ممکن است اثرات مخرب و جبران‌ناپذیری بر امنیت اقتصادی و توانمندی‌های دفاعی کشورها برجای گذارد، از اینرو اهمیت شناخت تهدیدات، آسیب‌پذیری‌ها و یافتن راهکارهای تدافعی و بهبود امنیت این سامانه‌ها بیش از پیش احساس می‌شود.

به‌طور کلی برقراری امنیت در بخش‌های مختلف یک زیرساخت صنعتی در سالیان متمادی یکی از بخش‌های اساسی کارفرمایان، پیمانکاران، مهندسين و بهره‌برداران صنایع بوده و به‌صورت گسترده تمام مسائل برنامه‌ریزی و بهره‌برداری سامانه‌های کنترل صنعتی را تحت تأثیر قرار داده است. در گذشته، این چالش‌ها بیشتر ناشی از خسارات وارده در اثر حریق، طغیان و خرابی‌های فیزیکی تجهیزات صنعتی بوده است، اما حرکت به سمت هوشمندسازی سامانه‌های کنترل صنعتی که ورود گسترده سامانه‌های اطلاعاتی، ارتباطی و کامپیوتری را در بر داشته، چالش‌های امنیتی جدیدی را در حوزه سایبری ایجاد کرده است. دلیل ایجاد این چالش‌های جدید امنیتی، وابستگی شدید سامانه‌های کنترل صنعتی به سامانه‌های اطلاعاتی و ارتباطی است که امنیت آن‌ها را به یکدیگر وابسته می‌کند.