۱۲۱۰۵۱

بسم الله الرحمن الرحیم

مرجع کاربردی

امنیت سایبری سامانه‌های کنترل صنعتی

(Industrial Control Systems Cyber Security)

نویسنده:

مهندس محمد عبدالتاجدینی

- 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: فیپا
- موضوع: کنترل فرایندها - پیش‌بینی‌های ایمنی
- موضوع: Process control - Security measures
- موضوع: کامپیوترها - ایمنی اطلاعات
- موضوع: Computer securi
- موضوع: سیستم‌های کنترل تطبیقی
- موضوع: Adaptive control systems
- موضوع: سامانه‌های کنترل با بازخورد - پیش‌بینی‌های ایمنی
- موضوع: Feedback control system - Security measures
- رده بندی کنگره: ۱۳۹۶ ۵م۲ع/TS۱۵۶/۸
- رده بندی دیویی: ۶۷۰/۴۲۷۵
- شماره کتابشناسی ملی: ۵۱۱۱۰۷۶

نشر ایده‌نگار ..... 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: **۸-۳۸-۸۳۰۴-۶۰۰-۹۷۸**|

نشانی مرکز پخش: تهران، میدان انقلاب، کوچه شهید رشتچی، پلاک۱۳، طبقه دوم، واحد ۴

فهرست مطالب

فصل دوم

امنیت در سازمان‌ها و زیرساخت‌های صنعتی

فصل سوم

تهدیدات و آسیب‌پذیری‌های سامانه‌های کنترل صنعتی

فصل چهارم

حملات سایبری در سامانه‌های کنترل صنعتی

دیباچه نویسنده

امروزه با حضور تجهیزات و سامانه‌های کنترلی مبتنی بر کامپیوتر[1] 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[2]ها و سامانه‌های DCS[3] و SCADA[4] مجهز شده‌اند؛ از طرفی هم‌اکنون با توسعه شبکه‌های کامپیوتری، تجهیزات و سامانه‌های فیلدباس 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. PLC‌ها، سامانه‌های DCS و SCADA به‌طور گسترده جهت کنترل و نظارت فرآیندهای صنعتی از جمله نفت، گاز، پتروشیمی، برق، هسته‌ای و دیگر صنایع بزرگ و کوچک مورد استفاده قرار می‌گیرند. پیشرفت‌های روزافزون در سامانه‌های کنترل صنعتی و تجهیزات مورد استفاده در آنها نه تنها باعث افزایش کارآیی و بهبود عملکرد سامانه‌ها و فرآیند شده، بلکه کنترل بسیاری از فرآیندهای ناممکن و یا پیچیده را تسهیل بخشیده و امکان کنترل و نظارت از راه دور را فراهم ساخته است. امروزه علی‌رقم 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

---

[1] منظور کنترل‌کننده‌های صنعتی می‌باشند که دارای ساختاری شبیه به کامپیوتر هستند.

[2] Programmable Logic Controller

[3] Distributed Control Systems

[4] 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 دغدغه‌های اساسی کارفرمایان، پیمانکاران، مهندسین و بهره‌برداران صنایع بوده و به‌صورت گسترده تمام مسائل برنامه‌ریزی و بهره‌برداری سامانه‌های کنترل صنعتی را تحت تاثیر قرار داده است. در گذشته، این چالش‌ها بیشتر ناشی از خسارات وارده در اثر حوادث طبیعی 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.