

بِسْمِ اللَّهِ الرَّحْمَنِ الرَّحِيمِ

پدافند سایبری سامانه و شبکه کنترل صنعتی

(معماری، پروتکل‌ها، آسیب‌پذیری‌ها، تهدیدات، مخاطرات
و راهکارهای مصون‌سازی سایبری)

۲۲۷۰۵۰۷ ✓
www.ketab311
تألیف و تصنیف:

دکتر علی ناصری

عضو هیأت علمی دانشگاه جامع امام حسین (علیه السلام)

دانشکده و پژوهشکده کامپیوتر، شبکه و ارتباطات

دانشگاه جامع امام حسین (علیه السلام)

مؤسسه چاپ و انتشارات



سرشناسه	ناصری، علی، ۱۳۴۸
عنوان و پدیدآور	پدافند سایبری سامانه و شبکه کنترل صنعتی (معماری، پروتکل‌ها، آسیب‌پذیری‌ها، تهدیدات، مخاطرات و راهکارهای مصون‌سازی سایبری) / تألیف و تصنیف: علی ناصری
مشخصات نشر	تهران: دانشگاه جامع امام حسین (ع) - مؤسسه چاپ و انتشارات، ۱۴۰۰
مشخصات ظاهری	بیست، ۴۰۰ ص.
فروست	دانشگاه جامع امام حسین (ع)، مؤسسه چاپ و انتشارات؛ ۱۰۳۰؛ سری سایبری-۱
شابک	۹۷۸-۶۲۲-۲۸۶-۰۷۰-۷
وضعیت فهرست‌نویسی	فیا
یادداشت	رمزگذاری داده‌ها ((Data encryption (Computer science))
موضوع	رمزنگاری (Cryptography)
موضوع	کامپیوترها -- ایمنی اطلاعات (Computer security)
موضوع	کامپیوترها -- کنترل دستیابی - رمزگان
موضوع	(Computers -- Access control -- Code words)
موضوع	فضای مجازی -- تدابیر ایمنی (Cyberspace -- Security measures)
شناسه افزوده	دانشگاه جامع امام حسین (ع) - مؤسسه چاپ و انتشارات
رده‌بندی کنگره	QA ۷۶/۹
رده‌بندی دیویی	۰۰۵/۸۲
شماره کتاب‌شناسی ملی	۸۷۲۱۱۱

کلیه حقوق، اعم از چاپ و تکثیر، نسخ‌برداری، ترجمه و اقتباس برای دانشگاه جامع امام حسین (ع) محفوظ است.

- عنوان: پدافند سایبری سامانه و شبکه کنترل صنعتی (معماری، پروتکل‌ها، آسیب‌پذیری‌ها، تهدیدات، مخاطرات و راهکارهای مصون‌سازی سایبری)
- تألیف و تصنیف: علی ناصری
- صفحه‌آرایی: ناهید آقامیرزایی
- طراح جلد: سعید عباسی
- ناظر فنی چاپ: حمید قمری
- لیتوگرافی، چاپ و صحافی: مرکز چاپ بلاغ
- نوبت چاپ: اول (بهمن ماه ۱۴۰۰)
- شمارگان: ۲۰۰ نسخه
- قیمت: ۱,۴۹۰,۰۰۰ ریال
- نشانی: تهران، بزرگراه شهید بابایی، بعد از پل لشکرک، دانشگاه جامع امام حسین (ع)، معاونت پژوهش و فناوری، مؤسسه چاپ و انتشارات، تلفن: ۷۴۱۸۸۲۶۰ دورنگار: ۷۴۱۸۸۲۷۴
- مرکز پخش: تهران، میدان فردوسی، فروشگاه و نمایشگاه مؤسسه چاپ و انتشارات دانشگاه جامع امام حسین (ع)، تلفن: ۸۸۸۳۹۲۹۷

بسم الله الرحمن الرحيم

«يُؤْتِي الْحِكْمَةَ مَنْ يَشَاءُ وَمَنْ يُؤْتَ الْحِكْمَةَ فَقَدْ أُوتِيَ خَيْرًا كَثِيرًا...»

حکمت را به هر کس بخواهد می‌دهد و کسی که به او حکمت داده شود، حقا خیری فراوان داده شده است...

(سوره مبارکه بقره - آیه ۲۶۹)

انقلاب کبیر اسلامی، نمونه‌ای بی‌بدیل تاریخی، از حرکت اجتماعی عظیمی است که با سرنگونی طاغوت و برپایی نظام مقدس جمهوری اسلامی، امیدهای فراوانی را در دل مستضعفان و آزادی‌خواهان جهان برای تحقق آرمان‌های بلند دولت اسلامی، جامعه اسلامی و درنهایت، تمدن بزرگ اسلامی پدید آورد. در این میان، نهادهای علمی، به‌ویژه دانشگاه‌ها، باید نقش کلیدی سوزن‌بانی و هدایت قطار پیشرفت و رشد جامعه در مسیر صحیح انقلابی را ایفا نمایند.

دانشگاه جامع امام حسین علیه السلام به عنوان «دانشگاه سازمانی سپاه در تراز انقلاب اسلامی» با شعار «تزکیه، جهاد علمی، دانشگاه تمدن‌ساز»، در کنار مسئولیت مهم انسان‌سازی و تربیت سربازان عصر ظهور، وظیفه تولید و نشر معارف پاسداری از انقلاب اسلامی را نیز برعهده دارد. در این راستا، معاونت پژوهش و فناوری دانشگاه به‌منظور تکمیل چرخه مدیریت دانش بومی با سه ویژگی «اسلامی بودن»، «روزآمدی» و «کارآمدی»، با هدف دستیابی به مرجعیت علمی، افتخار و تلاش دارد تا زمینه و بستری لازم برای اساتید و پژوهشگران محترم این عرصه را فراهم نماید. امید است در سایه الطاف بیکران الهی و با گسترش فعالیت‌های انتشاراتی مؤسسه چاپ و انتشارات دانشگاه جامع امام حسین علیه السلام، این رسالت خطیر تحقق یابد.

در پایان، بر روح ملکوتی معمار و رهبر کبیر انقلاب اسلامی، حضرت امام خمینی رحمته الله علیه و همچنین شهدای گرانقدر انقلاب اسلامی، دفاع مقدس و مدافعان حرم درود می‌فرستیم و با آرزوی سلامتی و توفیقات هرچه بیشتر مقام معظم رهبری، امام خامنه‌ای رحمته الله علیه و نیز خدمتگزاران اسلام و کشور، از اساتید، فرهیختگان و اهل نقد و نظر تقاضا داریم با ارائه نظرها و پیشنهادهای خود، ما را یاری فرمایند.

و من الله التوفیق و علیه التکلان

معاونت پژوهش و فناوری

دانشگاه جامع امام حسین علیه السلام

فهرست مطالب

صفحه

عنوان

پیشگفتار..... (نوزده)

فصل اول: مروری بر سامانه‌های کنترل صنعتی..... ۱

۱-۱- مقدمه..... ۱

۱-۱-۱- سیر تکاملی سامانه‌های کنترل صنعتی..... ۴

۲-۱- مقایسه سامانه‌های کنترل صنعتی و فناوری اطلاعات..... ۴

۳-۱- سامانه‌های کنترل صنعتی..... ۱۵

۱-۳-۱- بخش‌های صنعتی سامانه کنترل صنعتی و وابستگی متقابل آن‌ها..... ۱۵

۲-۳-۱- سامانه کنترل صنعتی و وابستگی‌های زیرساخت حیاتی..... ۱۷

۳-۳-۱- انواع مختلف سامانه‌های کنترل..... ۱۸

۴-۱- تحلیل مطالب فصل..... ۲۰

فصل دوم: معماری، اجزا و پروتکل‌های سامانه‌های کنترل صنعتی..... ۲۱

۱-۲- مقدمه..... ۲۱

۱-۱-۲- سامانه‌های اسکادا..... ۲۲

۲-۱-۲- سامانه‌های کنترل توزیع شده..... ۲۸

۳-۱-۲- توبولوژی‌های مبتنی بر کنترل‌کننده قابل برنامه‌ریزی..... ۳۱

۲-۲- اجزای سامانه کنترل صنعتی..... ۳۲

۳-۲- پروتکل‌های ارتباطی سامانه کنترل صنعتی..... ۳۵

۱-۳-۲- Modbus پروتکل..... ۳۷

۲-۳-۲- FOUNDATION Fieldbus پروتکل..... ۴۲

۳-۳-۲- Profinet و Profibus پروتکل..... ۴۴

۴-۳-۲- پروتکل رابط محرک/ حسگر..... ۴۷

۵-۳-۲- پروتکل مبدل از راه دور قابل آدرس‌دهی بزرگ راه (HART)..... ۴۷

۶-۳-۲- پروتکل DNP3 و IEC 60870..... ۴۸

۷-۳-۲- CAN bus پروتکل..... ۴۸

۴۹	۸-۳-۲ پروتکل صنعتی مشترک (CIP) و پروتکل Ethernet/IP
۵۲	۹-۳-۲ پروتکل OLE برای کنترل فرایند (OPC)
۵۲	۱۰-۳-۲ سایر پروتکل‌های صنعتی
۵۳	۱۱-۳-۲ پروتکل‌های IOT
۵۵	۴-۲ نحوه عملکرد سامانه‌های کنترل صنعتی
۵۷	۵-۲ ملاحظات طراحی سامانه کنترل صنعتی
۵۹	۶-۲ تحلیل مطالب فصل
۶۱	فصل سوم: بررسی سامانه‌های کنترل صنعتی مطرح در دنیا، مقایسه عملکردی

و امنیتی آن‌ها

۶۱	۱-۳ مقدمه
۶۲	۲-۳ شرکت زیمنس
۶۴	۱-۲-۳ ویژگی‌های شرکت زیمنس
۶۵	۲-۲-۳ امنیت و محصولات امنیتی زیمنس
۷۵	۳-۳ شرکت سیکور
۷۶	۱-۳-۳ ویژگی‌های شرکت سیکور
۷۷	۲-۳-۳ راه‌حل‌های امنیتی شرکت سیکور
۸۳	۴-۳ شرکت هانیول
۸۴	۱-۴-۳ ویژگی‌های شرکت هانیول
۸۵	۲-۴-۳ راه‌حل امنیت سایبری شرکت هانیول
۸۹	۳-۴-۳ محصولات امنیتی شرکت هانیول
۹۱	۵-۳ شرکت اشنایدر الکتریک
۹۱	۱-۵-۳ ویژگی‌های شرکت اشنایدر الکتریک
۹۲	۲-۵-۳ راه‌حل‌های امنیت سایبری شرکت اشنایدر الکتریک
۹۴	۳-۵-۳ محصولات امنیتی شرکت اشنایدر الکتریک
۹۸	۶-۳ شرکت ABB
۹۸	۱-۶-۳ ویژگی‌های شرکت ABB
۹۹	۲-۶-۳ راه‌حل‌های امنیت سایبری شرکت ABB
۱۰۱	۳-۶-۳ راه‌حل امنیتی ABB Ability
۱۰۳	۴-۶-۳ محصولات امنیتی شرکت ABB

۱۰۶	۷-۳- شرکت IBM
۱۰۶	۱-۷-۳- ویژگی‌های شرکت IBM
۱۰۷	۲-۷-۳- راه‌حل امنیت سایبری شرکت IBM
۱۱۰	۳-۷-۳- محصولات امنیتی شرکت IBM
۱۱۳	۸-۳- شرکت جنرال الکتریک
۱۱۳	۱-۸-۳- ویژگی‌های شرکت GE
۱۱۴	۲-۸-۳- راه‌حل امنیت سایبری شرکت GE
۱۱۶	۳-۸-۳- خدمات امنیتی شرکت GE
۱۱۶	۴-۸-۳- محصولات امنیتی شرکت GE
۱۱۹	۹-۳- شرکت اتوماسیون راکول
۱۱۹	۱-۹-۳- ویژگی‌های شرکت راکول
۱۲۰	۲-۹-۳- راه‌حل‌های امنیت سایبری شرکت راکول
۱۲۲	۳-۹-۳- محصولات امنیتی شرکت راکول
۱۲۵	۱۰-۳- شرکت الکتریک امرسون
۱۲۵	۱-۱۰-۳- ویژگی‌های شرکت امرسون
۱۲۷	۲-۱۰-۳- راه‌حل‌های امنیتی شرکت امرسون
۱۲۸	۳-۱۰-۳- خدمات امنیت سایبری شرکت امرسون
۱۲۹	۴-۱۰-۳- محصولات امنیت سایبری شرکت امرسون
۱۳۱	۱۱-۳- شرکت یوگواوا
۱۳۱	۱-۱۱-۳- ویژگی‌های شرکت یوگواوا
۱۳۲	۲-۱۱-۳- راه‌حل‌های امنیتی شرکت یوگواوا
۱۳۴	۳-۱۱-۳- امنیت و ایمنی با OpreX شرکت یوگواوا
۱۳۵	۱۲-۳- راهکارهای امنیتی
۱۳۹	۱۳-۳- تحلیل مطالب فصل
۱۴۳	فصل چهارم: تهدیدات، آسیب‌پذیری‌ها و حملات سایبری سامانه‌های کنترل صنعتی
۱۴۳	۱-۴- مقدمه
۱۴۴	۲-۴- رویکردهای تحلیل امنیت سایبری سامانه کنترل صنعتی
۱۴۶	۳-۴- آسیب‌پذیری‌های سامانه کنترل صنعتی
۱۴۹	۱-۳-۴- پایگاه CVE

۱۵۸	۴-۳-۲- پایگاه CWE
۱۶۱	۴-۳-۳- پایگاه NVD
۱۶۲	۴-۴- آسیب پذیری های مورد سوءاستفاده در سامانه کنترل صنعتی
۱۶۷	۴-۵- دسته بندی آسیب پذیری های سامانه کنترل صنعتی
۱۷۲	۴-۵-۱- پایگاه ICS-CERT
۱۷۸	۴-۶- بررسی آسیب پذیری های رایج مؤلفه های مختلف سامانه کنترل صنعتی شرکت زیمنس
۱۸۲	۴-۷- تحلیل آماری آسیب پذیری های سامانه کنترل صنعتی
۱۸۳	۴-۷-۱- تجزیه و تحلیل آسیب پذیری ها در مؤلفه های سامانه کنترل صنعتی
۱۸۸	۴-۷-۲- دسترس پذیری مؤلفه های سامانه کنترل صنعتی در اینترنت
۱۹۱	۴-۸- تهدیدات سایبری سامانه های سامانه کنترل صنعتی
۱۹۷	۴-۸-۱- چالش های امنیت سایبری در سامانه کنترل صنعتی
۱۹۸	۴-۸-۲- تهدیدات امنیت سایبری در سامانه کنترل صنعتی
۲۰۵	۴-۹- حملات سایبری
۲۰۶	۴-۹-۱- معیارهای دسته بندی حملات سامانه کنترل صنعتی
۲۰۷	۴-۹-۲- تأثیرات بالقوه حملات سایبری بر مؤلفه های سامانه کنترل صنعتی
۲۰۸	۴-۹-۳- حملات سایبری متداول
۲۱۰	۴-۹-۴- حملات مهم بر زیرساخت های حیاتی
۲۱۳	۴-۱۰- تحلیل مطالب فصل
۲۲۹	فصل پنجم: مدیریت ریسک سامانه های کنترل صنعتی
۲۲۹	۵-۱- مقدمه
۲۲۹	۵-۲- مبانی و مفاهیم ریسک و مدیریت ریسک
۲۳۳	۵-۳- مدیریت ریسک
۲۳۴	۵-۳-۱- سامانه های مدیریت ریسک
۲۳۵	۵-۳-۲- پاسخ به ریسک
۲۳۶	۵-۳-۳- برنامه اضطراری
۲۳۶	۵-۳-۴- اهداف مدیریت ریسک
۲۳۶	۵-۳-۵- چگونگی انجام مدیریت ریسک
۲۳۸	۵-۳-۶- مفاهیم پایه ای مدیریت ریسک پروژه
۲۳۹	۵-۳-۷- فعالیت ها و خروجی های مدیریت ریسک

۲۴۰	۸-۳-۵- تعیین مسئولیت‌ها در مدیریت ریسک
۲۴۲	۳-۵-۹- فرایند تجزیه و تحلیل ریسک
۲۴۲	۵-۳-۱۰- پاسخگویی به ریسک
۲۴۳	۵-۴- تبیین چارچوب‌های مدیریت ریسک
۲۴۳	۵-۴-۱- چارچوب‌های مدیریت ریسک
۲۴۳	۵-۴-۲- چارچوب مدیریت ریسک NIST 800-37
۲۴۵	۵-۴-۳- چارچوب مدیریت ریسک ISO 31000
۲۵۱	۵-۵- تبیین مدل‌های مدیریت ریسک
۲۵۳	۵-۵-۱- مدل مدیریت ریسک حلزونی
۲۵۴	۵-۵-۲- مدل مدیریت ریسک SEI
۲۵۵	۵-۵-۳- مدل Soft risk
۲۵۶	۵-۶- تبیین و تشریح فرایندها و اکوسیستم مدیریت ریسک
۲۵۶	۵-۶-۱- فرایند مدیریت ریسک NIST
۲۶۰	۵-۶-۲- فرایند مدیریت ریسک ISO
۲۶۸	۵-۶-۳- فرایند مدیریت ریسک IT governance
۲۶۹	۵-۷- مکانیسم‌های ارزیابی ریسک در سامانه کنترل صنعتی
۲۷۱	۵-۷-۱- ایمنی در ارزیابی ریسک امنیت اطلاعات سامانه کنترل صنعتی
۲۷۲	۵-۷-۲- تأثیرات فیزیکی بالقوه یک حادثه سامانه کنترل صنعتی
۲۷۳	۵-۸- جدول ریسک
۲۷۴	۵-۸-۱- تأثیرات ریسک
۲۷۵	۵-۸-۲- احتمال ریسک
۲۷۵	۵-۸-۳- نقشه ریسک
۲۷۵	۵-۸-۴- اصلاحات
۲۷۹	۵-۹- نمونه‌ها و مثال‌های مدیریت و ارزیابی ریسک سایبری در سامانه کنترل صنعتی
۲۷۹	۵-۹-۱- چارچوب مدیریت ریسک عمومی اسکادا
۲۸۰	۵-۹-۲- دامنه چارچوب مدیریت ریسک عمومی اسکادا
۲۸۱	۵-۹-۳- مزیت این چارچوب و روش مشترک
۲۸۱	۵-۱۰- تحلیل مطالب فصل

فصل ششم: استانداردها و مقررات سامانه‌های کنترل صنعتی	۲۸۳
۱-۶- مقدمه	۲۸۳
۲-۶- استانداردها و مقررات مشترک	۲۸۵
۳-۶- استاندارد ISA/IEC-62443	۲۹۲
۴-۶- روش ایده‌آل صنعت برای اداره کردن سامانه کنترل صنعتی	۲۹۵
۵-۶- معیارهای مشترک و استانداردهای FIPS	۳۰۲
۶-۶- راهنمای NIST SP 800-82 امنیت سامانه‌های کنترل صنعتی	۳۰۴
۷-۶- ISA-99- امنیت اتوماسیون صنعتی و کنترل سامانه امنیتی	۳۰۶
۸-۶- IEC 62443- شبکه‌های ارتباطی صنعتی و امنیت سامانه	۳۰۷
۹-۶- تحلیل مطالب فصل	۳۰۷
فصل هفتم: پدافند سایبری سامانه‌های کنترل صنعتی	۳۱۵
۱-۷- مقدمه	۳۱۵
۲-۷- محدودیت‌های امنیتی سامانه کنترل صنعتی	۳۱۷
۳-۷- سیاست‌ها و رویه‌ها	۳۱۹
۴-۷- مدل دفاع در عمق	۳۲۲
۵-۷- شناسایی دارایی‌ها	۳۲۶
۶-۷- شناسایی ریسک	۳۳۰
۷-۷- ارزیابی ریسک	۳۳۲
۸-۷- مدیریت امنیت در IT و OT	۳۳۲
۹-۷- معماری امنیتی سامانه کنترل صنعتی	۳۳۴
۱-۹-۷- تقسیم‌بندی و تفکیک شبکه	۳۳۵
۲-۹-۷- محافظت از مرز	۳۳۸
۳-۹-۷- فایروال‌ها	۳۴۱
۴-۹-۷- شبکه کنترل از نظر منطقی جدا	۳۴۵
۵-۹-۷- تفکیک شبکه	۳۴۶
۶-۹-۷- معماری دفاع در عمق توصیه شده	۳۵۳
۷-۹-۷- دروازه‌های یک طرفه	۳۵۵
۸-۹-۷- افزونگی و تحمل خطا	۳۵۶
۹-۹-۷- جلوگیری از حملات مرد میانی	۳۵۷

پیشگفتار

با گسترش و پیشرفت روزافزون صنایع، شاهد رشد و پیشرفت چشمگیر سامانه‌های کنترل صنعتی هستیم. سامانه‌های کنترل صنعتی هسته اصلی یک مجموعه صنعتی است؛ لذا شناخت این سامانه‌ها و محافظت و تأمین امنیت آن‌ها، نیاز به مطالعه، برنامه‌ریزی و طراحی اقدامات مناسب دارد. امروزه فناوری‌های نوین حوزه فناوری اطلاعات و ارتباطات تحول عظیمی در سامانه و زیرساخت‌های کنترل صنعتی به وجود آورده است. به همان نسبت که سامانه‌های کنترل صنعتی از این فناوری‌های استفاده می‌کنند توجه کشورها در جنگ‌ها، برای اختلال و تخریب آن‌ها افزایش می‌یابد. یکی از مهم‌ترین تهدیدات برای امنیت ملی کشورها، اختلال و تخریب در زیرساخت حیاتی کشور منجمله دیسپاچینگ برق، دیسپاچینگ گاز، شبکه کنترل راه‌آهن، شبکه‌های نیروگاهی و پالایشگاهی و زیرساخت‌های صنعتی و کنترلی بخش دفاعی است. با توجه به حجم تهدیدات علیه زیرساخت‌ها و سامانه‌های کنترل صنعتی، توسعه دانش مصون‌سازی سایبری آن‌ها بسیار با اهمیت است. موضوع مصون‌سازی در دو قالب امنیت و تاب‌آوری مطرح است. بررسی حملات سایبری گزارش شده از مراجع معتبر جهانی حاکی از حجم بالای حملات در حوزه سامانه‌های کنترل صنعتی دارد. حوادث سایبری چند سال اخیر در ایران نیز نشان از توجه گروه‌های ساختار یافته و غیرساختار یافته سایبری به تخریب و اختلال در این سامانه‌ها دارد. مصون‌سازی سایبری این سامانه‌ها در مقابل حملات سایبری مستلزم تسلط علمی و دانشی بر معماری، استانداردها و اجزاء

آن‌ها و همچنین تکنیک‌ها و روش‌های مصون‌سازی آن‌ها می‌باشد. در این راستا، کتاب حاضر با هدف ارتقاء سطح شناخت سامانه‌های کنترل صنعتی و تسلط بر اصول، تکنیک‌ها و روش‌های مصون‌سازی آن‌ها تألیف گردید. این کتاب با رویکرد رفع نیازهای این حوزه، برای اساتید، دانشجویان، محققین و همچنین بهره‌برداران سامانه‌های کنترل صنعتی تدوین شده است. امید آن داریم این کتاب در ارتقاء سطح مصون‌سازی زیرساخت‌های حیاتی کشور تأثیرگذار باشد. ضمناً نویسنده با آغوش باز پذیرای نظرات و پیشنهادات خوانندگان گرامی خواهد بود تا در چاپ‌های آتی مدنظر قرار گیرند.

علی ناصری

www.ketab.ir