

امنیت صنعتی

همگرایی سایبر-فیزیکی

IT در برابر OT

چرا امنیت سایبری در محیط عملیاتی متفاوت است؟

تحلیل فلسفی، معماری و ابزاری و پیامدهای آن برای امنیت سایبری صنعتی

محمد حسن ابراهیمی
رئیس کمیته امنیت اتوماسیون صنعتی

اگر یک سیستم برای یک ساعت از کار بیفتد، چه رخ می‌دهد؟

پیامد در OT

- 🔥 توقف کامل خط تولید
- 🔥 آسیب فیزیکی به ماشین‌آلات
- ⚠️ خطر جانی و زیست‌محیطی

پیامد در IT

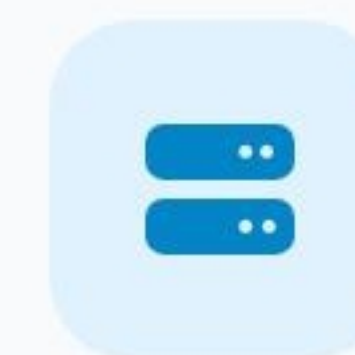
- ❗ اختلال موقت در سرویس
- ❗ نارضایتی موقت کاربران
- ❗ بازیابی نسبتاً سریع داده‌ها

یک «قطعی» در این دو محیط هرگز معنای یکسانی ندارد.



دنیای فرآیندها (OT)

سیستم‌های PLC، SCADA و ماشین‌آلات.
کنترل رفتار فیزیکی و مادی جهان واقعی.



دنیای داده‌ها (IT)

سرورها، نرم‌افزارها، شبکه‌های سازمانی.
مدیریت جریان اطلاعات و تعامل کاربران دیجیتال.

در IT، امنیت یعنی حفاظت از سرویس و اطلاعات.

در OT، امنیت یعنی حفاظت از ایمنی و فرآیند فیزیکی.

روش‌های تغییر متفاوت

ابزارهای متفاوت

معماری‌های متفاوت

اولویت‌های متفاوت

تفاوت در تعریف «دارایی»

دارایی در OT

ایمنی انسان و محیط زیست

خط تولید و ماشین‌آلات

استمرار فرآیند عملیاتی

دارایی در IT

داده و اطلاعات محرمانه

حساب‌های کاربری

سرورها و سرویس‌های ابری

تفاوت در اولویتهای امنیتی

مدل عملیاتی (Safety First)

۱ ایمنی (Safety & Reliability)

۲ استمرار فرآیند (Availability)

۳ یکپارچگی فرمان (Integrity)

مدل سایبری (CIA)

۱ محرمانگی (Confidentiality)

۲ یکپارچگی (Integrity)

۳ دسترس پذیری (Availability)

تفاوت در معنای «محرمانگی»

در OT محرمانگی مهم است، اما:

- ⚠️ نباید مانع دسترسی اپراتور به وضعیت شود
- ⚠️ دیده شدن فرآیند برای ایمنی الزامی است
- ⚠️ کنترل محلی بر پنهان سازی اولویت دارد

در IT افشا باعث می شود:

- ✓ نشت اطلاعات حساس مشتریان
- ✓ سرقت اسرار تجاری سازمان
- ✓ پیامدهای شدید قانونی و اعتباری

تفاوت در معنای «یکپارچگی»



در OT

فرمان‌ها و مقادیر فرآیند تغییر نکنند.

مثال: تغییر مخرب فشار، دما، یا سرعت موتور.



در IT

داده بدون تغییر غیرمجاز باقی بماند.

تفاوت در معنای «دسترس پذیری»

در OT

Downtime = حادثه

در IT

Downtime = هزینه

هر ساعت توقف در صنایع کلیدی = صدها میلیون تا میلیاردها تومان زیان + خطر ایمنی.

تفاوت در معماری شبکه

OT برای کنترل ساخته شده

- ✓ ساختار لایه‌ای و تفکیک شده
- ✓ پردازش محلی قطعی (Edge)
- ✓ ارتباطات ثابت و ایستا
- ✓ دفاع کم‌ریسک بدون اختلال فرآیند

IT برای اتصال ساخته شده

- ✓ ارتباطات گسترده و اینترنت
- ✓ سرویس‌های متمرکز ابری
- ✓ آدرس‌دهی پویا و کاربران متغیر
- ✓ دفاع تهاجمی و مسدودسازی سریع

تفاوت در چرخه حیات و تغییر

شاخص	محیط IT	محیط OT
چرخه عمر	۳ تا ۵ سال (سریع).	گاهی ۱۵ تا ۳۰ سال (طولانی).
نصب و صله	مداوم و معمولاً خودکار.	فقط در پنجره‌های توقف مجاز.
راه‌اندازی مجدد	قابل قبول در بیشتر سرویس‌ها.	بسیار خطرناک برای فرآیند.

مدل معماری صنعتی (Purdue) و مرزهای امنیتی

هرچه به پایین نزدیک می‌شویم، تحمل تغییر و اختلال کمتر می‌شود.

دسترسی بالا

سطح ۴ و ۵: شبکه‌های سازمانی (IT)

سطح ۳.۵: منطقه غیرنظامی (Industrial DMZ)

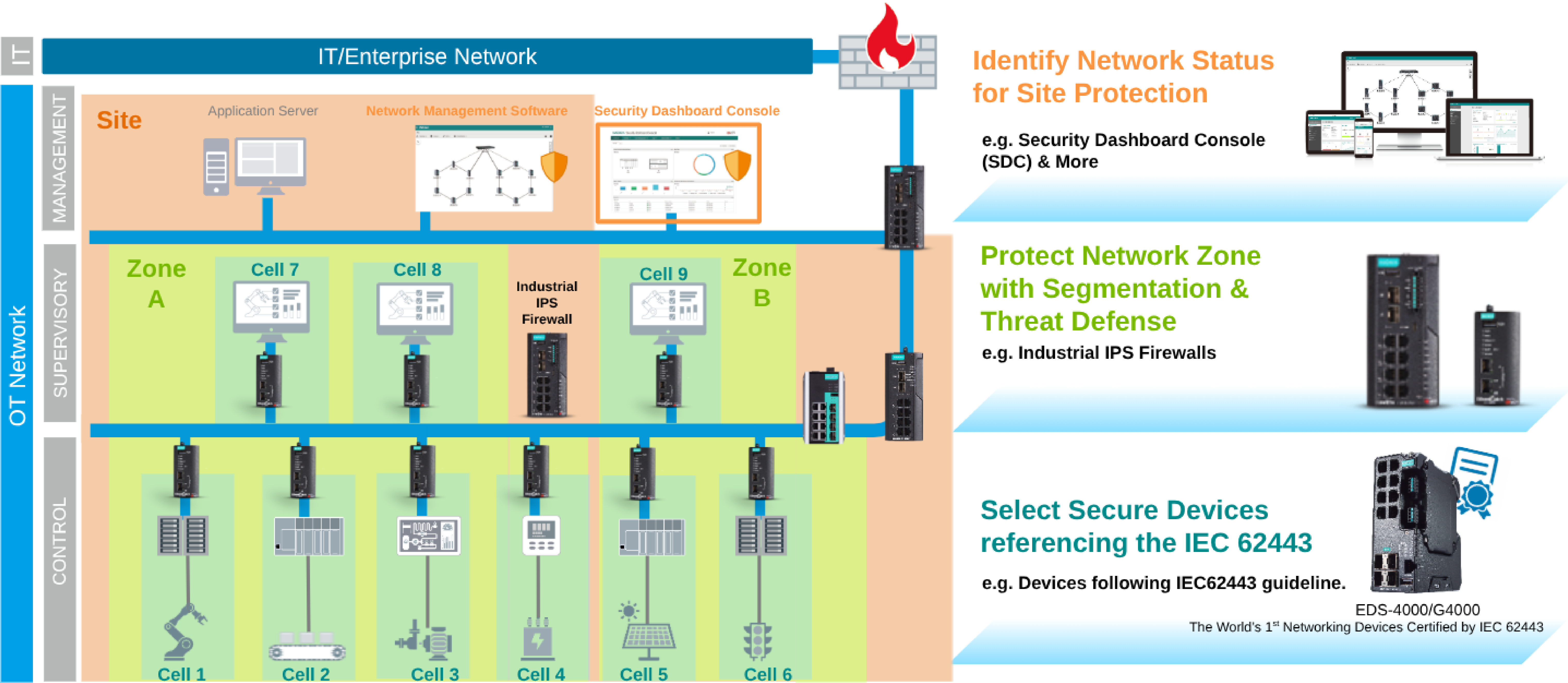
سطح ۳: مدیریت عملیات (SCADA / MES)

سطح ۱ و ۲: کنترل‌گرهای محلی (PLC / RTU)

دسترسی ایزوله

سطح ۰: فرآیند فیزیکی و ماشین‌آلات

Defense-in-depth Approach & Solution Design



تفاوت در پروتکل‌ها

پروتکل‌های صنعتی

Modbus, DNP3, OPC UA

- ⚠️ اغلب فاقد رمزنگاری ذاتی
- ⚠️ احراز هویت بسیار ضعیف
- ⚠️ طراحی‌شده برای شبکه‌های ایزوله

پروتکل‌های سازمانی

TCP/IP, HTTP, DNS, API

- ✓ استانداردسازی بالا
- ✓ پشتیبانی از رمزنگاری مدرن
- ✓ احراز هویت قوی

تفاوت در رفتار ترافیک شبکه

ترافیک OT: قابل پیش بینی

فرآیند محور، تکرارشونده و حساس به تأخیر زمانی.
تشخیص تهدید: از طریق انحراف از خط مبنا.

ترافیک IT: متغیر

وابسته به رفتار انسانی، نوسانی و دارای حجم متغیر.
تشخیص تهدید: عمدتاً از طریق امضاهای حمله.

نگاه متفاوت به دسترسی از راه دور

در OT: یک استثنای کنترل شده

- فقط در صورت ضرورت مطلق
- محدود به زمان مشخص (موقت)
- از طریق Jump Server و ضبط جلسات
- نیازمند تأیید فیزیکی اپراتور محلی

در IT: یک روال عادی

دسترسی VPN برای کارکنان دورکار یک استاندارد پذیرفته شده و دائمی است.

تفاوت در ابزارهای دفاعی

حوزه فعالیت	رویکرد در IT	رویکرد در OT
کشف دارایی	اسکن فعال شبکه.	شنود غیرفعال (Passive).
امنیت نقاط انتهایی	آنتی ویروس و EDR تهاجمی.	محدودسازی اجرا (Whitelisting).
پایش وقایع	SIEM بر اساس لاگ سرورها.	پایش با درک محتوای صنعتی.



چرا اسکن فعال در OT خطرناک است؟

اختلال در ارتباطات بلادرنگ.

افزایش ناگهانی بار پردازشی.

توقف کنترل‌گرهای قدیمی
(PLC).

رمزنگاری در OT ممنوع نیست؛

اما باید مهندسی شود.

سازگاری پروتکل‌های صنعتی

ظرفیت پردازشی تجهیزات

بررسی تأخیر ارتباطی

دسترسی در شرایط اضطراری

امنیتی که فرآیند را ناامن کند، امنیت موفق نیست.

تفاوت در تمرکز تیم‌ها

تیم OT محافظت می‌کند از:

- تداوم و پایداری تولید
- سلامت ماشین‌آلات
- ایمنی فیزیکی پرسنل کارخانه

تیم IT محافظت می‌کند از:

- پایگاه‌های داده و اطلاعات
- شبکه‌های ارتباطی سازمانی
- هویت و دسترسی کاربران

تصمیم امنیتی OT بدون حضور تیم بهره‌برداری، تصمیم کاملی نیست.

تفاوت در چارچوب‌ها و استانداردها

حوزه OT

IEC 62443

NIST SP 800-82

NERC CIP

حوزه IT

ISO/IEC 27001

NIST CSF

الزامات حریم خصوصی (GDPR)

در محیط عملیاتی (OT) هرگز نباید:

✗ بدون ارزیابی، اسکن فعال شبکه انجام داد.

✗ به روزرسانی خودکار ویندوز را فعال کرد.

✗ سیستم کنترل را مستقیماً به اینترنت متصل کرد.

✗ خارج از پنجره مجاز، تغییری ایجاد کرد.

✗ ابزار امنیتی IT را بدون تست در OT نصب کرد.

✗ اثر تغییر سایبری بر ایمنی را نادیده گرفت.

در محیط عملیاتی (OT) همیشه باید:

✓ دارایی‌ها و ارتباطات را دقیق شناسایی کرد.

✓ شبکه را از طریق Industrial DMZ جداسازی کرد.

✓ ترافیک را به صورت غیرفعال پایش کرد.

✓ دسترسی راه دور را محدود و ضبط کرد.

✓ وصله‌ها را پیش از اجرا در محیط مشابه تست کرد.

✓ تصمیمات را مشترکاً با تیم بهره‌برداری گرفت.

سناریو: کشف آسیب پذیری در SCADA

تفاوت در سرعت نیست؛ تفاوت در مدیریت پیامد است.

راهکار مسئولانه OT

۱. آزمون در محیط آزمایشگاهی مشابه
۲. تهیه نسخه پشتیبان برای بازگشت
۳. هماهنگی پنجره توقف با بهره برداری
۴. اجرای کنترل شده و پایش دقیق

راهکار عجولانه IT

۱. دانلود و نصب فوری وصله
۲. راه اندازی مجدد سرور
۳. خطر توقف ناگهانی خط تولید!

امنیت OT، نسخه صنعتی امنیت IT نیست.

باید مبتنی بر ارزیابی ریسک باشد.

باید فرآیند محور باشد.

باید با کمترین اختلال اجرا شود.

باید ایمنی فیزیکی را تضمین کند.

پرسش پایانی

به چه میزان از ابزارها و روش های IT می توان در محیط OT استفاده کرد؟

سپاسگزارم از توجه شما

جهت دسترسی به فایل های پرزنتیشن اسکن کنید

