

ناوک هوشمند پویان

Edge Intelligent Enterprise

امنیت سایبری شبکه های کنترل صنعتی (OT / SCADA)

فایروال صنعتی بومی

ویژه صنعت برق

www.navak-ai.ir

امنیت پایدار برای زیرساخت های حیاتی برق

1.	ضرورت امنیت سایبری در صنعت برق	2
2.	معرفی راهکار فایروال صنعتی بومی	3
3.	چالش‌ها و تهدیدات شبکه‌های OT	4
4.	لزوم استقرار فایروال صنعتی و IDS/IPS در پست‌های برق مناطق مرزی کشور	5
5.	معماری امنیت صنعتی مبتنی بر IEC 62443	7
6.	تحلیل رفتار پروتکل‌های صنعتی و IDS/IPS	8
7.	کنترل فعال ترافیک OT با فایروال صنعتی	10
8.	حفاظت از پروتکل‌های صنعتی صنعت برق	11
9.	سخت‌افزارهای صنعتی مورد استفاده	13
10.	انطباق با استانداردها و الزامات امنیتی	15
11.	ویژگی‌های محیطی و قابلیت اطمینان	17
12.	سناریوهای کاربردی (Use Cases)	18
13.	جمع‌بندی و ارزش پیشنهادی راهکار	19
14.	منابع	
15.	جدول مشخصات فنی مدل‌ها	

امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



1. ضرورت امنیت سایبری در صنعت برق

شبکه‌های کنترل صنعتی در صنعت برق، ستون فقرات عملیات تولید و توزیع انرژی محسوب می‌شوند. هرگونه اختلال یا حمله سایبری به این شبکه‌ها می‌تواند پیامدهای گسترده‌ای از جمله توقف تولید، کاهش کیفیت خدمات، خسارت‌های مالی و حتی تهدید ایمنی افراد به دنبال داشته باشد. به همین دلیل، امنیت سایبری در صنعت برق نه یک گزینه، بلکه یک ضرورت حیاتی است.

شبکه‌های (Operational Technology) OT که کنترل فرآیندها و تجهیزات را بر عهده دارند، با شبکه‌های IT متفاوت هستند. این شبکه‌ها نیازمند قابلیت اطمینان بالا، تأخیر کم و عملکرد مداوم هستند، اما در عین حال در برابر تهدیدات سایبری بسیار آسیب‌پذیرند. عواملی مانند توپولوژی ضعیف شبکه، نقاط ورود بدون محافظ، تجهیزات آسیب‌پذیر مانند PLC و RTU، رایانه‌های شخصی وصله نشده و خطاهای انسانی می‌توانند راه نفوذ هکرها یا بدافزارها را هموار کنند.

افزون بر این، پیچیدگی و تنوع پروتکل‌های صنعتی و ارتباط میان لایه‌های مختلف شبکه، خطرات را دوجندان می‌کند. حتی یک دستور غیرمنتظره یا تغییر ناگهانی در رفتار تجهیزات می‌تواند به توقف فرآیندها و اختلال در ایمنی منجر شود. بنابراین، مدیریت و حفاظت همه‌جانبه از ترافیک صنعتی و کنترل دستورات، به عنوان یک نیاز اساسی برای تضمین تداوم عملیاتی و ایمنی، ضروری است.

راهکارهای امنیتی معمول IT قادر به پاسخگویی به این تهدیدات نیستند، زیرا این سیستم‌ها فقط IP و پورت‌ها را تحلیل می‌کنند و از درک رفتار واقعی تجهیزات صنعتی عاجزند. از سوی دیگر، یک راهکار تخصصی برای OT با بهره‌گیری از بازرسی عمیق بسته‌ها (DPI) و سیستم‌های IDS/IPS صنعتی قادر است فرامین واقعی پروتکل‌ها را تحلیل کرده و رفتار غیرعادی را شناسایی و کنترل نماید. این قابلیت، پایه‌ای برای محافظت هوشمند، فعال و قابل دفاع شبکه‌های برق است.

در این میان، سامانه‌های تشخیص نفوذ (IDS) و جلوگیری از نفوذ (IPS) در شبکه‌های عملیاتی صنعت برق، نقشی فراتر از ابزارهای امنیتی متداول ایفا می‌کنند. این سامانه‌ها با تمرکز بر تحلیل رفتار واقعی پروتکل‌های صنعتی و فرمان‌های کنترلی، قادرند تهدیدات پنهان، دستورات غیرمجاز و حملات هدفمند را پیش از ایجاد اختلال عملیاتی شناسایی و مهار نمایند.

در شبکه برق، IDS/IPS نه صرفاً یک راهکار فنی، بلکه یک سازوکار حیاتی برای حفظ پایداری شبکه، ایمنی تجهیزات و جلوگیری از خاموشی‌های گسترده محسوب می‌شود.

در نتیجه، سرمایه‌گذاری در یک راهکار امنیتی OT نه تنها به کاهش ریسک‌های سایبری کمک می‌کند، بلکه اعتماد بهره‌برداران، بهره‌وری شبکه و ایمنی عملیاتی را تضمین می‌نماید و سازمان را قادر می‌سازد الزامات استانداردهای بین‌المللی و ملی را به سادگی برآورده کند.



ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



2. معرفی راهکار فایروال صنعتی بومی

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، به طور ویژه برای شبکه‌های کنترل صنعتی صنعت برق طراحی شده است تا امنیت سایبری را به صورت جامع و فعال فراهم کند. این راهکار، ترکیبی از تجهیزات سخت‌افزاری مقاوم در محیط‌های صنعتی و نرم‌افزار تحلیل ترافیک پیشرفته است که به شما امکان می‌دهد شبکه OT را با دقت بالا محافظت نمایید.

با بهره‌گیری از بازرسی عمیق بسته‌ها (Deep Packet Inspection)، این راهکار قادر است محتوای فرمان‌ها و پروتکل‌های صنعتی را تحلیل کرده و هرگونه رفتار غیرعادی، دستورات غیرمجاز یا تهدیدات بالقوه را شناسایی نماید. این توانمندی فراتر از فایروال‌های IT عمل می‌کند و کنترل دقیقی بر رفتار تجهیزات و فرامین شبکه فراهم می‌آورد.

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، قابلیت‌های متعددی را در یک دستگاه یکپارچه ارائه می‌دهد: مدیریت ترافیک شبکه، NAT، VPN صنعتی با رمزنگاری سخت‌افزاری، و سیستم پیشگیری از نفوذ (IPS). همچنین، این راهکار از پروتکل‌های متداول صنعتی شامل Modbus TCP/RTU، OPC Classic، UA، DNP3، IEC104، S7 و Ethernet/IP پشتیبانی می‌کند و امکان افزودن پروتکل‌های جدید در به‌روزرسانی‌های آتی فراهم است.

ویژگی مهم دیگر، انعطاف‌پذیری در پیکربندی و مدیریت سیاست‌های امنیتی است. با تشخیص هوشمند پروتکل‌های صنعتی، امکان ایجاد Policy‌های دقیق و ساده برای هر بخش از شبکه فراهم شده است، بدون آنکه نیاز به پیچیدگی‌های فنی زیاد باشد. این قابلیت باعث کاهش زمان راه‌اندازی و بهبود قابلیت اطمینان عملیاتی می‌شود.

از لحاظ زیرساختی، فایروال صنعتی بومی ناوک هوشمند پویان، در دو نوع Rack-mounted و Track-mounted عرضه می‌شود که امکان نصب در محیط‌های مختلف صنعتی، از داخل تابلو برق روی خط تولید تا اتاق کنترل و مانیتورینگ را فراهم می‌کند. مقاومت بالا در برابر دما، رطوبت و گرد و خاک، پشتیبانی از پاور Redundant و امکان Bypass کردن فایروال در مواقع ضروری، تضمین می‌کند که حتی در شرایط بحرانی، فرآیند صنعتی بدون وقفه ادامه یابد.

در مجموع، این راهکار با ترکیب سخت‌افزار صنعتی مقاوم، تحلیل هوشمند پروتکل‌های صنعتی، مدیریت متمرکز سیاست‌های امنیتی و قابلیت اطمینان بالا، یک لایه حفاظتی قابل اعتماد، هوشمند و فعال برای شبکه‌های برق ایجاد می‌کند و پایه‌ای محکم برای برآورده کردن الزامات استانداردهای بین‌المللی و ملی در حوزه امنیت سایبری OT فراهم می‌سازد.

امنیت سایبری
شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



3. چالش ها و تهدیدات شبکه های OT

شبکه های کنترل صنعتی در صنعت برق با چالش های خاصی مواجه هستند که بدون محافظت مناسب می توانند پیامدهای عملیاتی و ایمنی جدی به همراه داشته باشند. این شبکه ها برخلاف شبکه های IT، نیازمند عملکرد پایدار، تأخیر کم و اطمینان بالا هستند، اما در عین حال در برابر تهدیدات سایبری بسیار آسیب پذیرند.

مهم ترین چالش ها و نقاط ضعف شبکه های OT :

1. سیستم ها و تجهیزات قدیمی (Legacy Systems) : بسیاری از PLC ها، RTU ها و تجهیزات شبکه، فاقد به روزرسانی های امنیتی هستند و به راحتی می توانند مورد حمله قرار گیرند.
2. توبولوجی ضعیف و نقاط ورودی بدون محافظ: دسترسی های غیرمجاز یا ارتباطات ناامن بین تجهیزات و شبکه های IT، می تواند راه نفوذ مهاجمین را باز کند.
3. خطای انسانی و مدیریت ناصحیح: تنظیمات نادرست، استفاده از رمز عبور ضعیف، یا اتصال دستگاه های غیرمجاز به شبکه، تهدیدات سایبری را افزایش می دهد.
4. دسترسی از راه دور و رایانه های وصله نشده: اتصال مهندسان، پیمانکاران یا تجهیزات خارجی بدون کنترل و رمزنگاری مناسب، یکی از مسیرهای اصلی نفوذ است.
5. تنوع و پیچیدگی پروتکل های صنعتی: شبکه های برق از پروتکل های متنوعی استفاده می کنند (Modbus, OPC, DNP3, IEC104, S7) و تحلیل و کنترل صحیح ترافیک بدون ابزار تخصصی دشوار است.
6. آسیب پذیری در برابر حملات عملیاتی و ایمنی: یک دستور غیرمجاز یا رفتار غیرعادی تجهیزات می تواند به توقف خطوط تولید، خاموشی های ناگهانی یا خطر برای پرسنل منجر شود.

ضرورت استقرار فایروال صنعتی و IDS/IPS در پست های مرزی

یکی از نقاط پریسک در شبکه برق کشور، پست ها و مراکز کنترلی مستقر در مناطق مرزی هستند. این نقاط به دلیل ارتباطات مخبراتی، نزدیکی جغرافیایی و مسیرهای تبادل داده، بیش از سایر بخش ها در معرض حملات سایبری فرامرزی قرار دارند. استقرار فایروال صنعتی مجهز به IDS/IPS در این پست ها، امکان کنترل دقیق ترافیک، شناسایی رفتارهای غیرعادی و جلوگیری از نفوذ هدفمند را فراهم می کند و نقش مهمی در حفاظت از شبکه سراسری برق و امنیت انرژی کشور ایفا می نماید.

کشورهای مورد هدف قرارگرفته حملات سایبری برق

تجربیات بین المللی نشان می دهد که شبکه های برق در کشورهای مختلف هدف حملات سایبری سازمان یافته قرار گرفته اند. از جمله می توان به خاموشی های گسترده ناشی از حملات سایبری در اوکراین، تلاش برای نفوذ به زیرساخت های برق ایالات متحده، حملات ثبت شده به شبکه های انرژی در آلمان و اختلالات سایبری در شبکه برق مناطق مرزی هند اشاره کرد. این نمونه ها نشان می دهد که حمله به شبکه برق، به یکی از ابزارهای فشار راهبردی در سطح منطقه ای و بین المللی تبدیل شده است.

پیام کلیدی:

شبکه های OT بدون راهکار امنیتی تخصصی، تنها به صورت واکنشی عمل می کنند و حتی ابزارهای استاندارد IT قادر به شناسایی تهدیدات خاص تجهیزات صنعتی نیستند. برای حفاظت واقعی، نظارت فعال، تحلیل رفتار پروتکل ها و کنترل دقیق فرمان های صنعتی ضروری است.



4. لزوم استقرار فایروال صنعتی و IDS/IPS در پست‌های برق مناطق مرزی کشور

تهدیدات خاص پست‌های برق مناطق مرزی

پست‌های برق واقع در مناطق مرزی به دلیل شرایط جغرافیایی و عملیاتی، در معرض تهدیدات سایبری بیشتری نسبت به مناطق داخلی قرار دارند، از جمله:

- ارتباط با شبکه‌ها یا پیمانکاران برون‌مرزی
 - افزایش احتمال دسترسی فیزیکی یا موقت مهاجمان
 - عبور ترافیک کنترلی از مسیرهای ارتباطی کم‌امن‌تر
- ✦ این شرایط، پست‌های مرزی را به نقاط ورودی بالقوه برای حملات هدفمند سایبری تبدیل می‌کند.

نقش فایروال صنعتی در حفاظت شبکه برق

فایروال‌های صنعتی به‌طور خاص برای محیط‌های OT/ICS طراحی شده‌اند و نقش کلیدی در موارد زیر دارند:

- کنترل و محدودسازی ترافیک غیرمجاز
- اعمال سیاست‌های امنیتی بر پروتکل‌های صنعتی (Modbus، DNP3، IEC 61850)
- تفکیک منطقی شبکه (Network Segmentation)
- کاهش سطح حمله (Attack Surface)

✦ عدم استفاده از فایروال صنعتی می‌تواند منجر به:

- اسکن و سوءاستفاده از پروتکل‌های کنترلی
- اختلال در فرمان‌ها و فرآیندهای حیاتی
- قطع سرویس یا تغییر غیرمجاز دستورات کنترلی شود.

نقش IDS/IPS در تشخیص و جلوگیری از حملات

- IDS با پایش مداوم ترافیک، رفتارهای غیرعادی و مشکوک را شناسایی کرده و هشدارهای امنیتی صادر می‌کند.

- IPS علاوه بر تشخیص، به‌صورت فعال حملات را مسدود و از گسترش آن‌ها جلوگیری می‌کند.

✦ این سامانه‌ها در مقابله با:

- حملات جعل فرمان
 - حملات انکار سرویس (DoS)
 - انتشار بدافزار در شبکه OT
- نقش حیاتی دارند.

اهمیت ویژه استقرار در پست‌های برق مرزی

شبکه برق به‌عنوان یکی از زیرساخت‌های حیاتی کشور (CII)، هرگونه اختلال در آن می‌تواند:

- خدمات عمومی حیاتی را تحت تأثیر قرار دهد
- خسارات اقتصادی و امنیتی گسترده ایجاد کند

در مناطق مرزی، احتمال حملات سایبری از مسیرهای خارجی افزایش یافته و نبود کنترل‌های امنیتی مناسب می‌تواند کل شبکه برق کشور را در معرض خطر قرار دهد.



فایروال صنعتی

بومی

ویژه صنعت برق

دفاع چندلایه (Defense in Depth)

ترکیب فایروال صنعتی با IDS/IPS یک معماری امنیتی چندلایه ایجاد می‌کند:

- فایروال → کنترل و محدودسازی دسترسی
 - IDS → شناسایی تهدیدات
 - IPS → جلوگیری فعال از حملات
- این ساختار باعث افزایش تاب‌آوری شبکه در برابر حملات پیشرفته می‌شود. ➤

انطباق با استانداردها

این رویکرد با الزامات استانداردهای نظیر **IEC 62443** و **NERC CIP** همخوانی کامل داشته و عدم پیاده‌سازی آن می‌تواند منجر به عدم انطباق و ریسک‌های عملیاتی جدی شود.

امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir

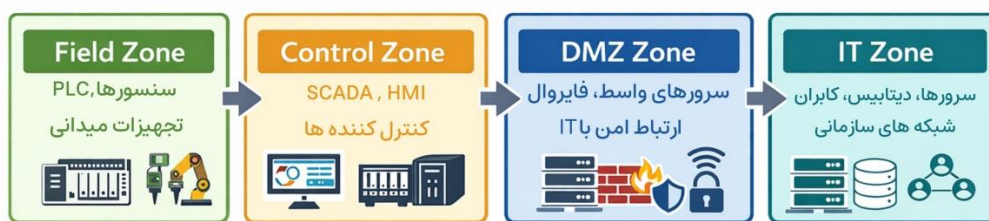


5. معماری امنیت صنعتی مبتنی بر IEC 62443

امنیت شبکه‌های کنترل صنعتی با ابزار شروع نمی‌شود؛ بلکه معماری صحیح شبکه و تفکیک لایه‌های حفاظتی اساس کار است. استاندارد بین‌المللی IEC 62443 یک چارچوب مرجع برای طراحی معماری امن OT ارائه می‌دهد که با استفاده از مفهوم **Zones & Conduits**، کنترل و مانیتورینگ شبکه را به صورت لایه‌به‌لایه ممکن می‌سازد.

ساختار معماری مرجع

- Field Zone**
شامل PLC ها و تجهیزات خط تولید است. دسترسی محدود و کنترل شده، تشخیص رفتار غیرعادی فرمان‌ها و Whitelisting فرامین ضروری است. این لایه کمترین دسترسی به IT و شبکه‌های مدیریتی را دارد و عملیات اصلی تولید در آن انجام می‌شود.
- Control Zone**
شامل SCADA ، HMI و تجهیزات مهندسی است. فایروال صنعتی و IDS/IPS در این لایه پیاده‌سازی می‌شوند تا ترافیک صنعتی کنترل شود. احراز هویت کاربران، محدود کردن نرخ فرمان‌ها و نظارت فعال، از ویژگی‌های این لایه است.
- DMZ (Demilitarized Zone)**
این لایه واسط میان شبکه OT و IT است و شامل Jump Server ، Historian و سایر سیستم‌های مانیتورینگ می‌شود. این بخش برای انتقال داده‌ها به شبکه IT امن شده و کنترل ترافیک در آن به دقت انجام می‌گیرد.
- IT Zone**
شامل سیستم‌های ERP ، ایمیل و اینترنت است. دسترسی به شبکه OT از این لایه محدود و کاملاً تحت نظارت فایروال و سیستم‌های IPS انجام می‌شود.



سه لایه دفاعی

- راهکار فایروال صنعتی بومی ناوک هوشمند پویان، امکان پیاده‌سازی دفاع در عمق سه‌وجهی را فراهم می‌کند:
- شبکه‌های مختلف صنعتی:** حفاظت از شبکه مدیریت، شبکه مانیتورینگ و شبکه خطوط تولید به صورت جداگانه و ایزوله.
 - زیرساخت‌های تجهیزات:** امکان قرارگیری فایروال بین PLC و ایستگاه مهندسی برای کنترل فرمان‌ها.
 - ترافیک پروتکل‌ها:** تحلیل و کنترل رفتار فرامین صنعتی برای شناسایی حملات احتمالی یا عملکرد غیرعادی.
- این ساختار امکان می‌دهد تا هر بخش از شبکه بر اساس سطح حساسیت و محل قرارگیری، محافظت شده و سیاست‌های امنیتی دقیق اعمال گردد.
- معماری IEC 62443 به سازمان کمک می‌کند تا امنیت پایدار، عملکرد بدون اختلال و انطباق با استانداردهای بین‌المللی را به طور همزمان داشته باشد.

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



6. تحلیل رفتار پروتکل های صنعتی و IDS/IPS

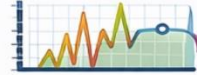
یکی از نقاط قوت کلیدی راهکار فایروال صنعتی بومی ناوک هوشمند پویان، توانایی تشخیص و تحلیل رفتار پروتکل های صنعتی است. برخلاف راهکارهای IT که تنها بر IP و پورت تمرکز می کنند، سیستم IDS/IPS صنعتی قادر است محتوای واقعی فرمان ها و دستورالعمل های تجهیزات را تحلیل نماید و فعالیت های غیرعادی را شناسایی کند.

آنچه IDS/IPS بررسی می کند:

- نوع دستور : فرامین Read ، Write و Control
- آدرس تجهیزات: PLC و RTU
- Register / Object Address
- نرخ غیرعادی فرمان ها و تغییر وضعیت ناگهانی
- حملات Replay یا Spoofing
- فرمان های خطرناک مانند STOP یا RESET

این تحلیل مبتنی بر رفتار واقعی فرایندها (Behavior-based) است و تنها به Signature های شناخته شده تکیه ندارد، بنابراین حتی تهدیدات ناشناخته نیز قابل شناسایی هستند.

IDS / IPS چه چیزی بررسی می کند؟

✓	فرامین: Read , Write و Control	  
✓	آدرس PLC و RTU	 
✓	Register / Object Address	 
✓	نرخ عادی فرمان ها و تغییر وضعیت ناگهانی	 
✓	حملات Spoofing یا Replay	  
✓	فرمان خطرناک مانند RESET یا STOP	 

امنیت سایبری

شبکه های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

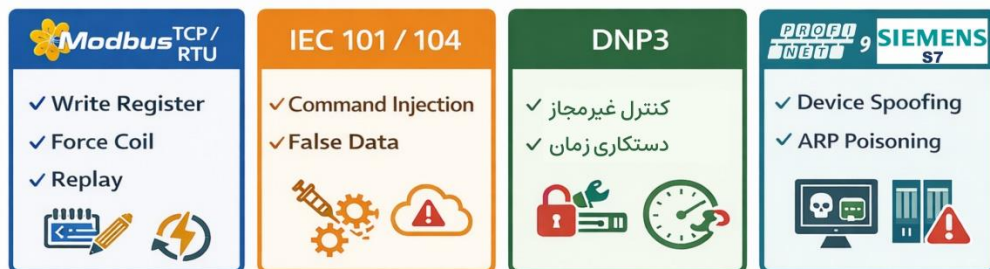
info@navak-ai.ir



قابلیت‌های DPI و پروتکل‌های پشتیبانی‌شده:

- **Modbus TCP/RTU** : شناسایی Write Register ، Force Coil و Replay
- **IEC 101/104**: Command Injection و False Data
- **DNP3** : کنترل غیرمجاز و دستکاری زمان
- **PROFINET و S7** : شناسایی Device Spoofing و ARP Poisoning

با این قابلیت، مدیر شبکه می‌تواند **Policy**های دقیق بر اساس رفتار تجهیزات صنعتی ایجاد کرده و ترافیک شبکه را به صورت فعال کنترل کند، بدون آنکه عملکرد تولید دچار اختلال شود.



پیام کلیدی:

- تحلیل رفتار پروتکل‌ها باعث کاهش خطرات عملیاتی و سایبری می‌شود
- سیستم IDS/IPS صنعتی، یک لایه حفاظتی فعال و هوشمند را ایجاد می‌کند
- ترکیب این تحلیل با معماری امن IEC 62443 ، یک راهکار جامع و مقاوم برای حفاظت از شبکه‌های OT ایجاد می‌کند

امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



7. کنترل فعال ترافیک OT با فایروال صنعتی

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، نه تنها شبکه را از تهدیدات خارجی محافظت می‌کند، بلکه کنترل فعال فرمان‌های صنعتی را نیز به‌طور مستقیم فراهم می‌آورد. این قابلیت به شما اجازه می‌دهد که ترافیک واقعی پروتکل‌های صنعتی را تحلیل و مدیریت کنید و از اجرای دستورالعمل‌های غیرمجاز جلوگیری نمایید.

ویژگی‌های کنترل فعال:

1. **Allow / Block بر اساس فرمان واقعی:**
امکان مسدودسازی یا اجازه عبور دستورهای مشخص بر اساس Function Code در پروتکل‌های صنعتی فراهم است.
2. **Passive Mode برای بررسی بدون اختلال:**
سیستم می‌تواند بدون تأثیر بر عملکرد شبکه، ترافیک را تحلیل کند و تهدیدات احتمالی را شناسایی نماید.
3. **Bypass و Fail-Safe :**
در مواقع بحرانی، فایروال می‌تواند از مدار خارج شود بدون اینکه جریان تولید متوقف گردد، تا تداوم عملیات تضمین شود.
4. **پیکربندی Policy های دقیق:**
ایجاد فیلترهای مبتنی بر IP ، Port و پروتکل صنعتی برای مدیریت هر بخش از شبکه به سادگی و با کمترین زمان.
5. **شناسایی و جلوگیری از رفتار غیرعادی:**
سیستم IDS/IPS صنعتی، رفتار تجهیزات و فرمان‌های عبوری را پایش می‌کند و هر تغییر غیرمنتظره یا فعالیت مشکوک را ثبت و متوقف می‌سازد.

پیام کلیدی:

- کنترل فعال فرمان‌ها، لایه حفاظتی عملیاتی و هوشمند را ایجاد می‌کند
- کاهش خطر توقف خطوط تولید، آسیب به تجهیزات و خطرات ایمنی
- امکان مدیریت متمرکز سیاست‌های امنیتی در سراسر شبکه‌های OT



8. حفاظت از پروتکل های صنعتی صنعت برق

در شبکه های OT صنعت برق، پروتکل های صنعتی ستون ارتباطات تجهیزات کنترل و مانیتورینگ هستند. هرگونه نفوذ یا رفتار غیرمجاز در این پروتکل ها می تواند به اختلال تولید، آسیب به تجهیزات و تهدیدات ایمنی منجر شود. راهکار فایروال صنعتی بومی ناوک هوشمند پویان، با تمرکز بر تحلیل رفتار ترافیک صنعتی و بازرسی عمیق بسته ها (DPI)، حفاظت فعال و هوشمند را فراهم می آورد.

تحلیل پروتکل ها به صورت عمیق و رفتارمحور

سیستم IDS/IPS داخلی قادر است:

- شناسایی دقیق دستورات هر پروتکل: از جمله Read/Write، System Command و Control
- ردیابی و ثبت Address تجهیزات (PLC/RTU) برای تشخیص دسترسی های غیرمجاز
- تحلیل Register / Object Address ها و شناسایی تغییرات غیرعادی یا دستورات Replay/Spoofing
- پایش نرخ فرمان ها و تغییرات State برای تشخیص اختلالات یا حملات DoS داخلی
- کنترل فرمان های بحرانی (STOP, RESET) و جلوگیری از اجرای ناخواسته آنها

پروتکل های صنعتی تحت پوشش

- Modbus TCP/RTU: تشخیص Write Register، Force Coil و Replay Attack
- IEC 101/104 و DNP3: جلوگیری از Command Injection و Time Manipulation
- OPC Classic / OPC UA و Ethernet/IP: شناسایی Device Spoofing و ARP Poisoning
- Siemens S7 و PROFINET: کنترل دقیق دستورات و پایش رفتار غیرعادی تجهیزات

مزیت های عملیاتی

- Behavior-based IDS/IPS: سیستم به رفتار واقعی فرایندها نگاه می کند و تنها به Signature های شناخته شده محدود نیست
- Policy های دقیق و قابل سفارشی سازی: ایجاد فیلترهای مبتنی بر IP، Port و پروتکل صنعتی برای هر Segment شبکه
- کاهش ریسک های داخلی و خارجی: کنترل فعال فرمان ها باعث کاهش خطر توقف خطوط تولید و اختلال عملیاتی می شود
- سازگاری با استاندارد IEC 62443: امکان پیاده سازی در چارچوب معماری امن و تفکیک Zones & Conduits

پیام کلیدی

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، با ترکیب تحلیل عمیق پروتکل ها، کنترل فعال فرمان ها و سیاست های متمرکز امنیتی، یک لایه حفاظتی پیشرفته و هوشمند برای شبکه های برق ایجاد می کند. این قابلیت، اطمینان می دهد که حتی در حضور حملات پیچیده یا تجهیزات آسیب پذیر، شبکه صنعتی به صورت پایدار، امن و قابل اعتماد باقی بماند.



فایروال صنعتی

بومی

ویژه صنعت برق

توضیحات تکمیلی	قابلیت کنترل فرمان‌ها	تهدیدات قابل شناسایی	قابلیت DPI	پروتکل صنعتی
کنترل دقیق دستورات خواندن و نوشتن، ثبت وقایع	فعال	Write Register ،Force Coil ، Replay Attack	بسیار بالا	Modbus TCP/RTU
شناسایی حملات تزریق فرمان، مدیریت دستورات بحرانی	فعال	Command Injection ،False Data	بسیار بالا	IEC 101/104
پایش زمان‌بندی و کنترل دسترسی‌های غیرمجاز	فعال	Unauthorized Control ، Time Manipulation	عالی	DNP3
شناسایی تجهیزات جعلی و صنعتی LAN محافظت از شبکه	فعال	Device Spoofing ،ARP Poisoning	بالا	PROFINET
پایش ترافیک داده‌های بین و تجهیزات SCADA	فعال	Unauthorized Read/Write ، Replay	بالا	OPC Classic / OPC UA
شناسایی دستورات غیرمجاز و PLC کنترل رفتار	فعال	Unauthorized Access ، Malformed Command	بالا	Siemens S7

امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



9. سخت افزارهای صنعتی مورد استفاده

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، بر اساس سخت افزارهای قدرتمند و مقاوم صنعتی طراحی شده است تا بتواند حفاظت جامع از شبکه های OT را در محیط های حساس و سخت صنعتی فراهم آورد. سخت افزارها با قابلیت های **Redundant**، مقاومت در برابر شرایط محیطی و پشتیبانی از پروتکل های صنعتی، ستون فقرات این راهکار را تشکیل می دهند.

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، شامل دو نوع Track-mounted و Rack-mounted می باشد. فایروال های صنعتی Rack-mounted از لحاظ دما و رطوبت و مقاومت در برابر گرد و خاک در درجه پایین قرار دارند و عموماً دارای فن می باشند به همین دلیل در مکان هایی مانند اتاق مانیتورینگ، کنترل و یا مکان هایی که دارای شرایط مناسب دما و رطوبت باشند قرار می گیرند و در داخل رک نصب می شوند. فایروال های صنعتی Track-mounted معمولاً مقاومت بالایی در برابر دما، رطوبت و گرد و خاک دارند و بدون فن می باشند و این قابلیت را دارند که مستقیماً در ZONE 0 بر روی خط تولید و یا داخل تابلو برق قرار گرفته و نصب شوند.

LEC-6032



- نوع دستگاه : Track-mounted
- پورت ها :

5 Combo Ethernet (10/100/1000 BaseT(X 1000/100 یا (Base SFP+)

- قابلیت های شبکه ای: Firewall، NAT، VPN، Router همه در یک دستگاه
- ویژگی های صنعتی:

- o دمای کاری: -40 تا +75 درجه سانتی گراد
- o دمای ذخیره سازی: -40 تا +80 درجه سانتی گراد
- o رطوبت: 5 تا 95 درصد بدون چگالش
- o پوسته تمام فلزی با استاندارد IP40

- قابلیت اطمینان: پاور Redundant، تکنولوژی Stateful Failover و Port Bypass
- سازگاری: پروتکل های صنعتی S7، IEC104، DNP3، OPC، Modbus و Ethernet/IP

امنیت سایبری
شبکه های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir





- نوع دستگاه: Rack-mounted برای اتاق کنترل و مانیتورینگ
- ویژگی‌های کلیدی:
 - o پردازنده قدرتمند با توان پردازش بالای بسته‌ها
 - o پشتیبانی از High Availability
 - o قابلیت مدیریت متمرکز و هماهنگ با IEC-6032
- ویژگی‌های محیطی:
 - o مقاومت مناسب در برابر دما و رطوبت (مکان‌های کنترل و رک‌های صنعتی)
 - o فن برای خنک‌کنندگی در محیط‌های بسته
- کاربرد: مناسب برای لایه‌های Control Zone و DMZ در معماری IEC 62443



- نوع دستگاه: پلتفرم پردازشی صنعتی Rack-mounted
- جایگاه در معماری: هسته امنیتی شبکه OT، DMZ و مراکز دیسپاچینگ
- قابلیت‌ها:
 - o توان پردازش بالا برای اجرای هم‌زمان فایروال صنعتی و IDS/IPS
 - o پشتیبانی از High Availability و سناریوهای Redundant
 - o مناسب برای شبکه‌های گسترده، چندسایته و پروژه‌های منطقه‌ای
- کاربرد:
 - o تجمیع امنیت چند پست برق
 - o پیاده‌سازی سیاست‌های امنیتی متمرکز
 - o حفاظت از ارتباط OT و IT در مقیاس کلان

پیام کلیدی:

- سخت‌افزارهای صنعتی انتخاب‌شده مقاوم، قابل اعتماد و با توان عملیاتی بالا هستند
- پشتیبانی از Redundancy و Port Bypass باعث تداوم عملیات بدون اختلال می‌شود
- ترکیب این سخت‌افزارها با قابلیت‌های نرم‌افزاری فایروال صنعتی، یک راهکار جامع، امن و عملیاتی برای شبکه‌های OT فراهم می‌کند



10. انطباق با استانداردها و الزامات امنیتی

در این راهکار امنیت سایبری صنعتی، انطباق با استانداردهای بین‌المللی به‌عنوان یک الزام اساسی در طراحی، پیاده‌سازی و بهره‌برداری در نظر گرفته شده است. ساختار کلی راهکار به‌گونه‌ای تدوین شده است که علاوه بر پاسخ‌گویی به تهدیدات سایبری محیط‌های عملیاتی صنعت برق، با چارچوب‌ها و الزامات پذیرفته‌شده جهانی در حوزه امنیت زیرساخت‌های حیاتی هم‌راستا باشد.

انطباق با استاندارد IEC 62443

این راهکار منطبق بر چارچوب امنیتی IEC 62443 طراحی شده است که به‌طور تخصصی برای حفاظت از سیستم‌های کنترل صنعتی (ICS) و زیرساخت‌های OT توسعه یافته است. در این چارچوب، مفاهیمی مانند تفکیک نواحی امنیتی (Zones)، کنترل ارتباطات بین نواحی (Conduits)، اصل حداقل دسترسی (Least Privilege) و مدیریت سطح دسترسی مبتنی بر نقش به‌صورت عملیاتی پیاده‌سازی شده‌اند. این انطباق باعث می‌شود ارتباطات بین تجهیزات حفاظتی، کنترلی و مانیتورینگ صنعت برق تنها در چارچوب سیاست‌های تعریف‌شده و تأییدشده مجاز باشد.

هم‌راستایی با استاندارد NERC CIP

در محیط‌های مرتبط با زیرساخت‌های حیاتی برق، الزامات NERC CIP نقش مهمی در مدیریت ریسک سایبری ایفا می‌کنند. این راهکار با تمرکز بر کنترل دسترسی، ثبت وقایع امنیتی، جداسازی شبکه‌های کنترلی از شبکه‌های سازمانی و پایش مداوم ترافیک، امکان پیاده‌سازی الزامات کلیدی این استاندارد را در سطح شبکه عملیاتی فراهم می‌کند. نتیجه این رویکرد، افزایش شفافیت امنیتی و کاهش احتمال نفوذ یا اختلال در سامانه‌های حیاتی برق است.

تطابق با چارچوب مدیریت امنیت اطلاعات ISO/IEC 27001

در لایه مدیریتی و فرآیندی، این راهکار با اصول ISO/IEC 27001 هم‌خوانی دارد. امکان ثبت رویدادها، مدیریت تغییرات، کنترل دسترسی کاربران، و پشتیبانی از سیاست‌های امنیت اطلاعات، به سازمان‌ها کمک می‌کند تا امنیت سایبری OT را در کنار امنیت IT، به‌صورت یکپارچه مدیریت نمایند.

انطباق با الزامات امنیتی ملی و گواهی افتا

این راهکار علاوه بر انطباق با استانداردهای بین‌المللی، دارای تأییدیه و گواهی امنیتی از مرکز مدیریت راهبردی افتا می‌باشد. وجود این گواهی نشان‌دهنده انطباق راهکار با الزامات امنیتی مصوب کشور برای استفاده در زیرساخت‌های حیاتی، شبکه‌های صنعتی حساس و سامانه‌های راهبردی صنعت برق است. دارا بودن گواهی افتا، امکان استفاده از این راهکار را در پروژه‌های دولتی، شرکت‌های تابعه وزارت نیرو، پست‌ها و نیروگاه‌ها فراهم کرده و ریسک حقوقی و امنیتی کارفرما را به‌طور قابل توجهی کاهش می‌دهد.



پایاده سازی رویکرد Defense in Depth

یکی از ارکان اصلی این راهکار، پایاده سازی دفاع در عمق (Defense in Depth) است. به جای اتکا به یک لایه امنیتی، ترکیبی از کنترل های شبکه ای، فایروال صنعتی، بازرسی عمیق پروتکل ها، محدود سازی فرمان های کنترلی و مانیتورینگ پیوسته به کار گرفته شده است. این رویکرد باعث می شود حتی در صورت عبور تهدید از یک لایه، لایه های بعدی مانع از تأثیرگذاری آن بر فرآیندهای حیاتی صنعت برق شوند.

آمادگی برای ممیزی و پروژه های سازمانی

طراحی این راهکار به گونه ای است که مستندات فنی، سیاست های امنیتی و ساختار پایاده سازی آن قابلیت ارائه در ممیزی های امنیتی، پروژه های EPC، مناقصات و طرح های توسعه ای صنعت برق را داشته باشد. این ویژگی، راهکار را به گزینه ای قابل اتکا برای سازمان های بهره بردار، شرکت های پیمانکار و نهادهای ناظر تبدیل می کند. و از نظر الزامات بومی و مقررات ملی، دارای گواهی افتا می باشد.

امنیت سایبری

شبکه های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



11. ویژگی های محیطی و قابلیت اطمینان

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، با هدف عملکرد پایدار در شرایط محیطی سخت و صنایع حساس طراحی شده است. سخت افزارهای LEC-6032 و NCA-4220 علاوه بر توان عملیاتی بالا، دارای ویژگی های محیطی و قابلیت اطمینان ویژه هستند که امنیت و استمرار عملیات شبکه های صنعتی برق را تضمین می کنند.

ویژگی های محیطی

- دامنه دمای کاری گسترده: از -40 تا +75 درجه سانتی گراد، مناسب محیط های گرم و سرد صنعتی
- دمای ذخیره سازی: از -40 تا +80 درجه سانتی گراد
- رطوبت عملیاتی: 5 تا 95 درصد بدون چگالش
- حفاظت در برابر گرد و غبار و ضربه: پوسته تمام فلزی با استاندارد IP40، مقاوم در برابر نفوذ اجسام بزرگتر از 1 میلیمتر
- سازگاری با محیط های Zone 0 و رک های کنترل صنعتی: Track-mounted برای خطوط تولید، Rack-mounted برای اتاق کنترل

قابلیت اطمینان

- Redundant Power: دو منبع تغذیه مستقل برای تضمین تداوم عملیاتی
- Stateful Failover و Port Bypass: امکان خروج فایروال از مدار بدون توقف فرایند و حفظ وضعیت شبکه
- High Availability (HA): پشتیبانی از ساختار فعال-فعال یا فعال-غیرفعال برای جلوگیری از قطعی شبکه
- کنترل دقیق تجهیزات: امکان پایش و مدیریت عملکرد سخت افزار و تشخیص خرابی ها پیش از تأثیرگذاری روی تولید

پیام کلیدی

- ترکیب مقاومت محیطی و قابلیت اطمینان عملیاتی، تضمین می کند که شبکه های OT حتی در شرایط بحرانی و محیط های سخت، امن و پایدار باقی بمانند
- این ویژگی ها، راهکار فایروال صنعتی ناوک را برای پروژه های حساس صنعت برق، نیروگاه ها و شبکه های کنترل بحرانی، یک گزینه ایده آل و قابل اعتماد می سازد

امنیت سایبری

شبکه های کنترل صنعتی

(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



12. سناریوهای کاربردی (Use Case)

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، با ترکیب سخت افزار مقاوم، تحلیل پروتکل ها و کنترل فعال فرمان ها، قابلیت پیاده سازی در محیط های مختلف شبکه های صنعتی برق را دارد. این سناریوها نمونه هایی از نحوه حفاظت شبکه، افزایش امنیت و کاهش ریسک های عملیاتی را نمایش می دهند.

سناریوی ۱: حفاظت از شبکه خطوط تولید (Field Zone)

- چالش: دسترسی غیرمجاز به PLC ها و تجهیزات میدان
- راهکار: نصب LEC-6032 Track-mounted روی خطوط تولید با DPI فعال برای Modbus, PROFINET, S7
- نتیجه: شناسایی و جلوگیری از دستورات خطرناک و غیرمجاز، کاهش ریسک توقف تولید و آسیب تجهیزات

سناریوی ۲: امنیت شبکه کنترل و SCADA (Control Zone)

- چالش: تهدیدات ناشی از کاربر یا تجهیزات مهندسی (Engineering Station)
- راهکار: NCA-4220 Rack-mounted با Policy های دقیق و کنترل فرمان ها، VPN امن برای دسترسی از راه دور
- نتیجه: حفاظت از SCADA و HMI در برابر Command Injection و Replay Attack، کنترل فعالیت کاربران و تجهیزات

سناریوی ۳: حفاظت از DMZ و شبکه مدیریت

- چالش: انتقال داده بین شبکه OT و IT بدون ایجاد آسیب امنیتی
- راهکار: فایروال صنعتی در DMZ با DPI و کنترل دستورات، مدیریت متمرکز گزارش ها و Logging
- نتیجه: جداسازی امن شبکه های OT و IT، کاهش ریسک حملات سایبری و حفاظت از اطلاعات حساس

سناریوی ۴: پروژه های بزرگ نیروگاهی و مراکز حساس

- چالش: شبکه های گسترده با تجهیزات متنوع و پراکنده
- راهکار: ترکیب LEC-6032 و NCA-4220 با قابلیت HA و Redundant Power، نصب در ZONE های مختلف
- نتیجه: استمرار عملیات، کنترل فعال فرمان ها، ایمنی تجهیزات و انطباق با استانداردهای IEC 62443 و NERC CIP

پیام کلیدی

- راهکار فایروال صنعتی ناوک انعطاف پذیر و مقیاس پذیر است و می تواند در انواع شبکه های برق از خطوط تولید کوچک تا نیروگاه های گسترده پیاده سازی شود
- تحلیل هوشمند پروتکل ها، کنترل فعال فرمان ها و معماری امن، امکان محافظت جامع از شبکه های OT را فراهم می کند.



13. جمع بندی و ارزش پیشنهادی راهکار

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، یک راه حل جامع امنیت سایبری برای شبکه های OT در صنعت برق است که با تمرکز بر واقعیت های عملیاتی، نیازهای فنی و الزامات استانداردهای بین المللی طراحی شده است. این راهکار تنها یک ابزار امنیتی نیست، بلکه بخشی از معماری دفاعی پایدار برای حفاظت از زیرساخت های حیاتی به شمار می رود.

جمع بندی فنی راهکار

- این راهکار با ترکیب مؤلفه های کلیدی زیر، امنیت شبکه های صنعتی را به صورت یکپارچه تأمین می کند:
- تحلیل عمیق و رفتارمحور پروتکل های صنعتی (DPI & IDS/IPS)
- شناسایی و کنترل فرمان های واقعی تجهیزات صنعتی به جای تکیه صرف بر Port و IP
- کنترل فعال فرمان های صنعتی (OT Firewall)
- جلوگیری از اجرای دستورات غیرمجاز، خطرناک یا غیرعادی بدون ایجاد اختلال در فرایند تولید
- سخت افزار صنعتی مقاوم و قابل اعتماد
- مبتنی بر تجهیزات صنعتی با قابلیت کار در شرایط محیطی سخت، High Availability و Redundancy
- انطباق با معماری و استانداردهای بین المللی
- طراحی منطبق با IEC 62443 و الزامات امنیتی صنعت برق، قابل استفاده در پروژه های حساس و بزرگ
- انطباق هم زمان با استانداردهای بین المللی و دارای گواهی افتا برای پروژه های دولتی و زیرساخت های حیاتی

ارزش پیشنهادی (Value Proposition)

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، برای سازمان های فعال در صنعت برق، ارزش های کلیدی زیر را ایجاد می کند:

- کاهش ریسک توقف تولید و خسارت عملیاتی
- با کنترل فعال فرمان ها و جلوگیری از حملات سایبری هدفمند
- افزایش ایمنی تجهیزات و فرایندها
- جلوگیری از دستورات خطرناک که می تواند منجر به آسیب فیزیکی یا حادثه شود
- قابلیت پیاده سازی تدریجی و مقیاس پذیر
- امکان استقرار در ZONE های مختلف شبکه بدون نیاز به تغییرات گسترده زیرساخت
- آمادگی برای ممیزی و پروژه های رسمی
- مستندسازی، Logging و انطباق با استانداردها برای پروژه های ملی و حساس
- یک راهکار بومی پذیر و پروژه محور
- متناسب با شرایط عملیاتی صنعت برق کشور و نیازهای واقعی بهره برداران
- این راهکار ریسک توقف ناگهانی شبکه برق را به صورت قابل اندازه گیری کاهش می دهد.

پیام نهایی

راهکار فایروال صنعتی بومی ناوک هوشمند پویان، پلی میان امنیت سایبری، پایداری عملیاتی و استانداردهای جهانی ایجاد می کند. این راهکار با رویکردی عملیاتی و مهندسی شده، سازمان ها را قادر می سازد تا شبکه های OT خود را به صورت ایمن، قابل اعتماد و آینده نگر محافظت کنند و با اطمینان وارد پروژه های بزرگ و حیاتی شوند.



نقش تجهیزات دارای گواهی IEC 61850-3 در ارتقای امنیت سایبری پست‌های برق هوشمند

تجربیات بین‌المللی نشان می‌دهد استفاده از تجهیزات صنعتی دارای گواهی IEC 61850-3، نقش کلیدی در تضمین پایداری عملیاتی و امنیت سایبری پست‌های برق اتوماتیک ایفا می‌کند. این رویکرد به‌ویژه در محیط‌های بدون اپراتور و مناطق حساس، به‌عنوان یک الزام فنی شناخته می‌شود.

کامپیوترهای دارای گواهی IEC 61850-3، توانمندساز امنیت سایبری در پست‌های برق خودکار



پیش‌زمینه

امنیت سایبری در پست‌های برق از اهمیت حیاتی برخوردار است؛ چرا که این پست‌ها به‌عنوان گره‌های کلیدی در شبکه برق، وظیفه توزیع انرژی الکتریکی به بخش‌های مختلف از جمله مناطق مسکونی، مراکز تجاری و خدمات حیاتی را بر عهده دارند. هرگونه نفوذ یا ضعف امنیتی در پست‌های برق می‌تواند نه‌تنها منجر به اختلال در تأمین برق شود، بلکه خطرات ایمنی جدی نیز به همراه داشته باشد. این خطرات شامل آسیب‌های فیزیکی احتمالی است که می‌تواند سلامت نیروی انسانی و حتی عموم مردم را تهدید کند. افزایش اتصال‌پذیری و دیجیتالی‌شدن شبکه برق، ریسک بروز اختلالات گسترده ناشی از حملات سایبری را به‌شدت افزایش داده است. در این میان، تجهیزات امنیت شبکه صنعتی در سطح سرور (Server-grade Industrial Network Security Appliances) با بهره‌گیری از قابلیت‌های سخت‌افزاری و نرم‌افزاری پیشرفته، امنیت شبکه پست‌های برق را تضمین می‌کنند. این تجهیزات به‌طور خاص برای پاسخ‌گویی به الزامات سخت‌گیرانه محیط‌های صنعتی حساس مانند پست‌های برق طراحی شده‌اند.

الزامات (Requirements)

یکی از یکپارچه‌سازان پیشرو در جنوب شرق آسیا که در حوزه اتوماسیون پست‌های برق فعالیت می‌کند، با چالش‌های جدی در حفاظت از زیرساخت‌های حیاتی خود در برابر تهدیدات روبه‌رشد سایبری مواجه شد. هرچند استفاده از فناوری‌های دیجیتال در پست‌های برق این مجموعه باعث افزایش بهره‌وری و بهبود کنترل شده بود، اما در عین حال آسیب‌پذیری‌هایی را نیز ایجاد کرده بود که می‌توانست مورد سوءاستفاده مهاجمان سایبری قرار گیرد. برای مقابله با این چالش‌ها، این یکپارچه‌ساز تصمیم گرفت یک راهکار جامع امنیت سایبری مبتنی بر سخت‌افزارهای شرکت لنر پیاده‌سازی کند. این راهکار باید الزامات زیر را برآورده می‌کرد:



گواهی نامه‌های IEC 61850-3 و IEEE 1613

محیط‌های زیرساخت حیاتی معمولاً شرایط سختی دارند؛ از جمله نوسانات ناگهانی دمای محیط، شوک و ارتعاشات مکانیکی و سایر عوامل خارجی. به همین دلیل، تجهیزات مورد استفاده در این محیط‌ها باید دارای گواهی‌های IEC 61850-3 و IEEE 1613 باشند تا استحکام و قابلیت اطمینان لازم برای استفاده در پست‌های برق را تضمین کنند.

دامنه دمای کاری گسترده

با توجه به دماهای بسیار بالا یا پایین در محیط‌های زیرساختی، سیستم‌های محاسباتی صنعتی مقاوم باید قادر باشند بدون کاهش ایمنی عملکرد یا بهره‌وری، در شرایط محیطی سخت به‌صورت پایدار کار کنند.

پشتیبانی از ورودی/خروجی‌های متنوع (Multiple I/O)

پلتفرم سخت‌افزاری مورد نظر باید از تعداد زیادی رابط I/O برای اتصال به کنتورها و رله‌ها پشتیبانی کند و همچنین دارای پورت‌های اترنت مناسب برای ارتباط با تجهیزات IED مبتنی بر استاندارد IEC 61850 باشد.

پشتیبانی گسترده از حافظه

تجهیزات سخت‌افزاری در پست‌های برق معمولاً حجم بالایی از داده تولید می‌کنند. برای تضمین یکپارچگی داده‌ها، استفاده از حافظه ECC (Error-Correcting Code) ضروری است. این نوع حافظه با تصحیح خطاهای حافظه، قابلیت اطمینان سیستم را در محیط‌های حساس پست برق به‌طور قابل توجهی افزایش می‌دهد.

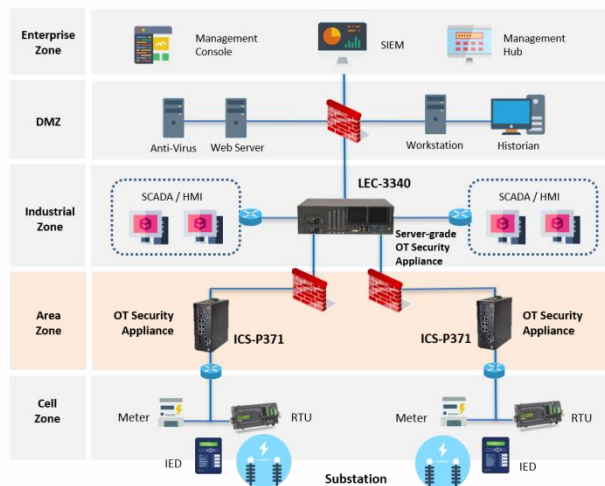
فناوری‌های امنیتی

وجود ماژول TPM 2.0 داخلی برای انجام پردازش‌های رمزنگاری امن و ایجاد مقاومت در برابر دستکاری فیزیکی در سطح سخت‌افزار، یکی از الزامات اصلی این راهکار امنیتی است.

منبع تغذیه افزونه (Redundant Power Supply)

برای تجهیزات مورد استفاده در صنعت برق، دسترس‌پذیری بالا و سهولت نگهداری اهمیت زیادی دارد. بنابراین، سیستم باید به منبع تغذیه پشتیبان مجهز باشد (AC+DC یا ورودی دوگانه DC) تا در زمان تعمیرات یا بروز اختلال در برق ورودی، عملکرد سیستم بدون وقفه ادامه یابد و از قطعی سرویس‌های شبکه جلوگیری شود.

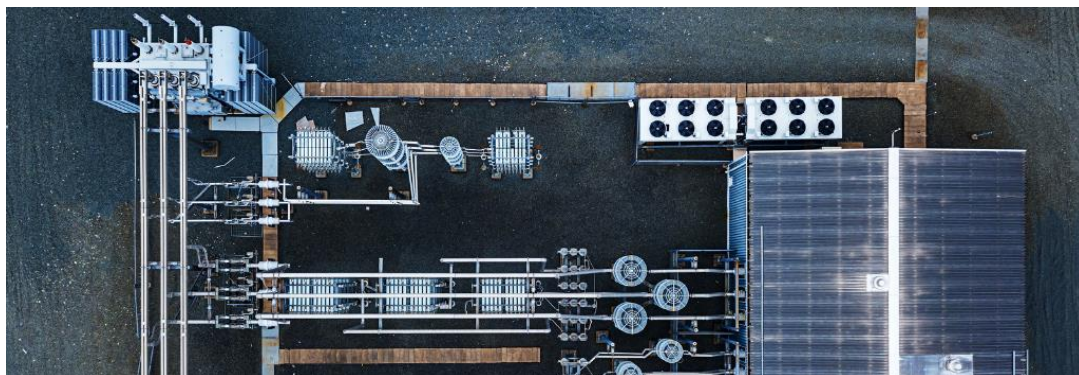
Ensuring Cybersecurity for Substation Automation



رله حفاظتی مجازی؛ گامی کلیدی در نوسازی و هوشمندسازی شبکه برق

در معماری‌های نوین شبکه برق، حرکت به سوی حفاظت نرم‌افزارمحور و مجازی‌سازی عملکردهای حفاظتی، به عنوان یکی از ارکان اصلی مدرن‌سازی شناخته می‌شود. این رویکرد ضمن افزایش انعطاف‌پذیری، امکان پیاده‌سازی کنترل‌های امنیتی پیشرفته و یکپارچه با زیرساخت OT را فراهم می‌کند.

رله حفاظتی مجازی برای نوسازی شبکه برق



پیش‌زمینه

رشد شهرنشینی، افزایش تقاضای انرژی و بالا رفتن هزینه‌ها، بیش از پیش بخش برق را به سمت استفاده هوشمندانه‌تر و کارآمدتر از ظرفیت‌های سیستم‌های الکتریکی سوق داده است؛ مسیری که به تحول پست‌های برق سنتی به پست‌های هوشمند منتهی می‌شود. نوسازی شبکه برق با سه چالش اصلی همراه است:

1. **تغییرات اقلیمی** که با ایجاد شرایط آب‌وهوایی شدید، پایداری شبکه برق را تحت تأثیر قرار می‌دهد.
 2. **افزایش ریسک حملات سایبری** علیه زیرساخت‌های شبکه برق.
 3. **نفوذ بالای منابع انرژی تجدیدپذیر** که موجب پیچیده‌تر شدن جریان‌های توان در شبکه می‌شود.
- مفهوم رله حفاظتی مجازی (**Virtual Protection Relay – VPR**) یکی از اجزای کلیدی در نوسازی شبکه برق به شمار می‌رود و راهکاری نوین برای حفاظت از پست‌های توزیع برق با ساختارهای پیچیده ارائه می‌دهد. این مفهوم با بهره‌گیری از معماری‌های مبتنی بر نرم‌افزار و پلتفرم‌های مجازی‌سازی، امکان پیاده‌سازی عملکردهای حیاتی حفاظت مدار را فراهم می‌کند. همچنین با ساده‌سازی مدیریت چرخه عمر تجهیزات، موجب افزایش کارایی، کاهش هزینه‌های سرمایه‌ای (CAPEX) و هزینه‌های نگهداری می‌شود و در نهایت، تأمین برق قابل اعتماد و تاب‌آور را برای آینده تضمین می‌کند.

الزامات

راهکار VPR می‌تواند با کاهش ابعاد فیزیکی و پیچیدگی زیرساخت پست برق، هزینه‌های سرمایه‌ای را کاهش داده و در عین حال انعطاف‌پذیری در پیاده‌سازی توابع حفاظتی و الگوریتم‌های اتوماسیون را افزایش دهد؛ امری که به بهبود عملکرد و کاهش هزینه‌های تعمیر و نگهداری منجر می‌شود. این راهکار مبتنی بر استاندارد IEC 61850 بوده و شامل الزامات کلیدی زیر است:

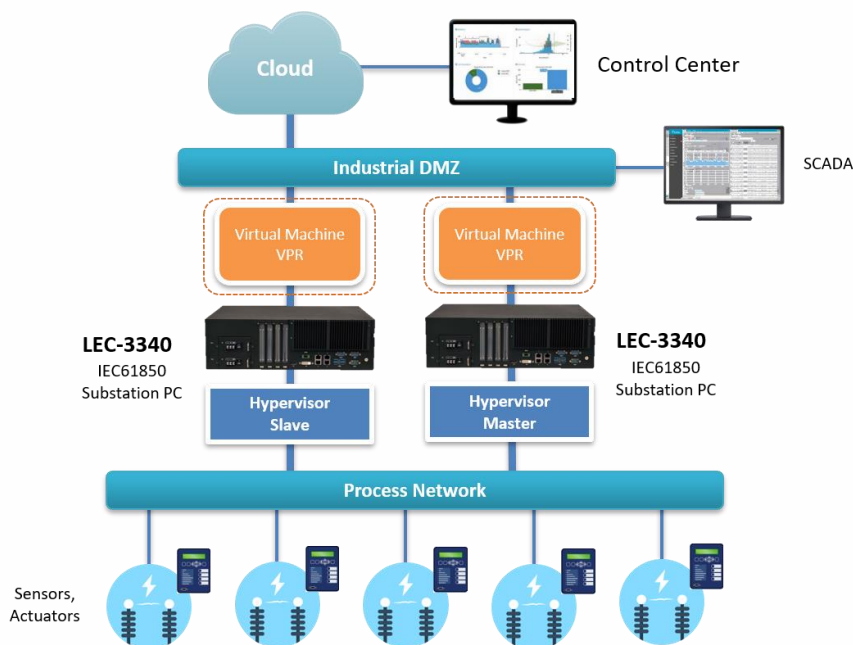
• گواهی‌های صنعتی مبتنی بر IEC

تجهیزات شبکه باید مطابق با استانداردهای IEC 61850-3 و IEEE 1613 باشند تا بتوانند شرایط سخت زیرساخت‌های حیاتی را تحمل کنند و به‌طور ویژه برای پست‌های برق طراحی شده باشند.



- **دسترسی پذیری بالا (High Availability)** : تأمین برق پایدار یک ضرورت اساسی است. وجود مسیر تغذیه برق افزونه (Redundant Power) امکان تداوم عملکرد و افزایش زمان در دسترس بودن سیستم را برای دوره‌های طولانی فراهم می‌کند.
- **مقیاس پذیری** : برخورداری از قابلیت‌های گسترده ورودی/خروجی (I/O)، امکان توسعه و افزایش ظرفیت برای پاسخ‌گویی به نیازهای رو به رشد، از جمله پشتیبانی از محفظه‌های درایو قابل تعویض، اسلات‌های PCIe برای کارت‌های هم‌زمان‌سازی زمانی و کارت‌های شبکه صنعتی (NIC) ضروری است.
- **امنیت سخت‌افزاری چندلایه** : وجود ماژول **TPM داخلی** برای انجام پردازش‌های رمزنگاری امن و ایجاد مقاومت در برابر دست‌کاری در سطح سخت‌افزار، یکی از الزامات مهم امنیتی این راهکار محسوب می‌شود.

Virtual Protection Relay for Power Grid Modernization



امنیت سایبری
شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



این مقاله توضیح می‌دهد برای محافظت کامل شبکه‌های OT (مثل شبکه‌های برق و IIoT)، باید امنیت چند لایه برقرار شود تا تهدیدات سایبری پیشرفته خنثی شوند. در این دیدگاه، ترکیب امنیت IT و OT و به کارگیری ابزارهای تخصصی مثل دیوارآتش صنعتی و سامانه تحلیل ترافیک پروتکل‌ها برای محافظت از تجهیزات حساس ضروری است.

خطر تهدیدات سایبری در شبکه‌های IIoT صنعتی



خطر تهدیدات سایبری در شبکه‌های IIoT صنعتی با سرعتی تاریخی افزایش یافته است، زیرا برنامه‌های IIoT مانند کارخانه‌های هوشمند، حمل‌ونقل هوشمند و شبکه‌های هوشمند برق (Smart Grid) به کمک پروتکل‌های شبکه معمولی متصل می‌شوند. حملات مخرب به‌طور فزاینده‌ای ویرانگرتر شده‌اند، از جمله کرم‌های Stuxnet، حملات DDoS، باج‌افزارها، تروجان‌ها و روش‌های نفوذ دیگر که می‌توانند از مسیرهای مختلف به شبکه‌های IIoT نفوذ کنند، هم در زیرساخت شبکه IT (فناوری اطلاعات) و هم در زیرساخت شبکه OT (فناوری‌های عملیاتی). برای حفاظت کامل شبکه‌های همگرا IIoT در برابر بدافزارهای پیشرفته، لازم است حفاظت‌های چندلایه‌ای برقرار شود که هر دو شبکه IT و OT را پوشش دهد، از جمله:

لایه صنعتی – (Industrial Zone) لایه ۰ تا ۳

این لایه شامل باس ابزار دقیق، شبکه LAN کنترلرها و سیستم‌های HMI و SCADA نظارتی است.

لایه DMZ صنعتی – (Industrial DMZ Zone) لایه ۳/۵

این لایه شبکه تبادل داده‌ها را شامل می‌شود، از جمله سرور ایمیل و سرورهای برنامه‌های کاربردی.

لایه سازمانی – (Enterprise Zone) لایه ۴ تا ۵

این لایه شبکه سازمانی را در بر می‌گیرد که شامل سرور وب، سرور ایمیل، سرور FTP و سرورهای سازمانی است.

امنیت سایبری
شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

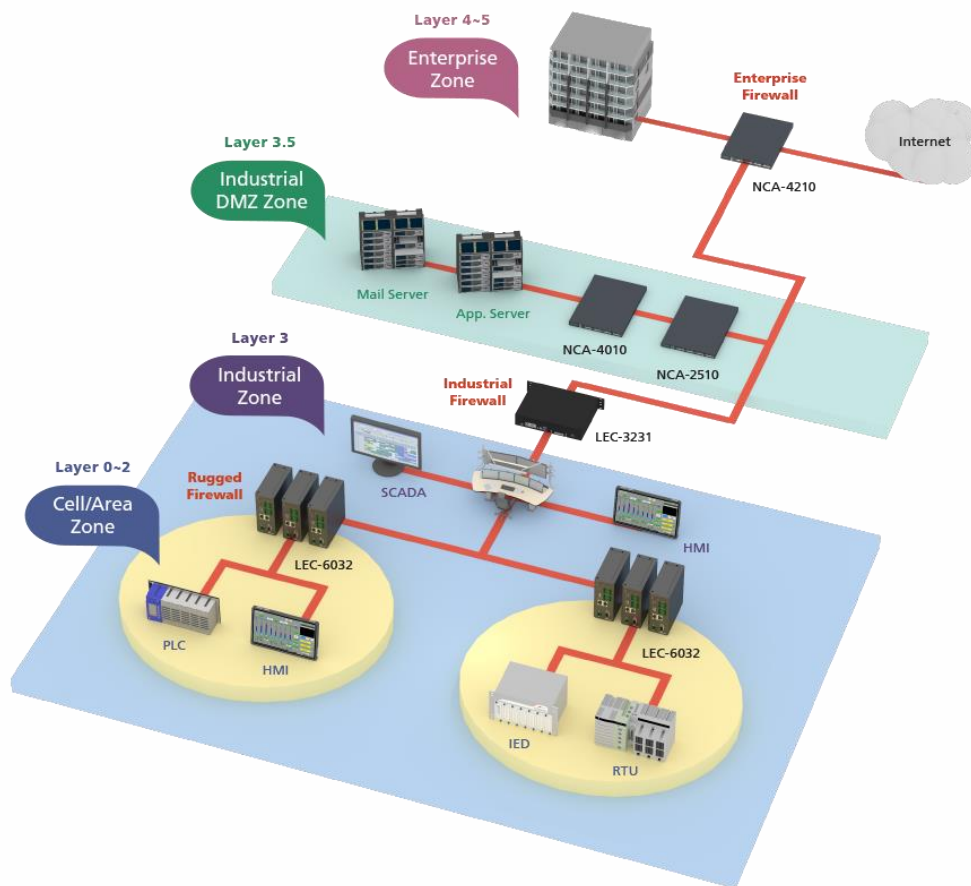
0933-6889690

www.navak-ai.ir

info@navak-ai.ir



فایروال صنعتی بومی ویژه صنعت برق



امنیت سایبری
شبکه های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



این مقاله تخصصی در حوزه صنعت برق و انرژی هست و درباره ترکیب و همگرایی امنیت IT و OT صحبت می‌کند و به نیاز به ابزار امنیت شبکه از جمله فایروال‌های صنعتی با کانفیگ LAN و پشتیبانی از کنترل ترافیک اشاره می‌کند.

تضمین امنیت سایبری صنعتی و همگرایی شبکه‌های IT و OT



پس‌زمینه

حدود اوت ۲۰۱۸، بزرگ‌ترین شرکت تولیدکننده نیمه‌هادی‌ها و پردازنده‌ها در تایوان مجبور شد به دلیل انتشار گسترده یک ویروس کامپیوتری، کارخانه‌های تولید خود را تعطیل کند. این تولیدکننده گزارش داد که برخی از سیستم‌های ساخت آن به نسخه مشتق‌شده ویروس واناکرای (WannaCry) آلوده شده‌اند؛ باج‌افزاری که در سال ۲۰۱۷ بسیاری از شرکت‌ها و مؤسسات را به شدت آسیب رساند.

اگرچه این شرکت بزرگ نیمه‌هادی به دلیل رعایت شدید پروتکل‌های امنیت IT شناخته شده بود، آسیب‌پذیری در حوزه فناوری عملیاتی (OT) کشف شد. این بخش در واقع با ارزش‌ترین بخش شرکت‌های تولید چیپ است، زیرا شامل دارایی‌ها و تجهیزات میلیون دلاری می‌شود. بنابراین حفاظت از OT ضروری است، زیرا این بخش تولید و خروجی محصولات را ایجاد می‌کند.

نیازمندی‌ها

یک شرکت پیشرو در امنیت سایبری صنعتی در منطقه EMEA به همراه شرکت لنر، مجموعه‌ای از راهکارهای نظارت و مدیریت شبکه را برای پرکردن شکاف بین IT و OT توسعه دادند. این راهکار مشترک باید سیستم‌های مستقر در محیط‌های SCADA، PLC و ICS (سیستم‌های کنترل صنعتی) را مدیریت، نظارت و کنترل کند تا از دسترسی و دستکاری تهدیدات سایبری جلوگیری شود. بنابراین، این گیتوی امنیت سایبری صنعتی باید دارای قابلیت‌های فوق باشد:



مطابقت با IEC/IEEE برای محیط‌های سخت

زیرساخت‌های حیاتی معمولاً در محیط‌های دورافتاده و بدون نگهدارنده با نوسانات برق یا عدم قطعیت‌های دیگر قرار دارند. بنابراین، راهکار ارائه شده باید با IEC61850-3 و IEEE1613 مطابقت داشته باشد تا اطمینان از پایداری فراهم شود.

بازرسی عمیق بسته‌ها (DPI)

DPI یکی از عناصر ضروری برای امنیت ICS است. این مکانیزم نه تنها بسته‌های شبکه را بررسی می‌کند، بلکه اطلاعات مفید (داده‌ها و متاداده‌ها) را برای نظارت بر شبکه‌های OT استخراج می‌کند.

توان پردازشی

توپولوژی هوش سایبری ممکن است با حجم بالای داده‌ها و DPI مواجه شود. بنابراین، راهکار مورد نیاز باید با پردازنده‌های با کارایی بالا و مصرف کم انرژی ساخته شود.

پیکربندی LAN غنی و انعطاف‌پذیر

برای فایروال صنعتی، پیکربندی LAN و پهنای باند حیاتی است. بنابراین، داشتن پیکربندی LAN غنی و انعطاف‌پذیر مانند چندین پورت GbE RJ45 برای مدیریت و پورت‌های SFP LAN ایده‌آل است.

مکانیزم LAN Bypass

LAN Bypass یک مکانیزم تحمل خطا ضروری، به‌ویژه برای سیستم‌های مستقر در محیط‌های دورافتاده و بدون نگهدارنده است. راهکار مورد نیاز باید با آخرین فناوری LAN Bypass یکپارچه شود تا پایداری ترافیک شبکه تضمین شود.

گسترش سیستم

زیرساخت شبکه که حوزه‌های IT و OT را به هم متصل می‌کند می‌تواند پیچیده باشد. بنابراین، ارائه امکان گسترش ماژول NIC برای افزایش پهنای باند و سایر عملکردهای مرتبط ایده‌آل است.

دامنه دمای عملیاتی وسیع

دمای محیطی شدید ممکن است در زیرساخت‌های حیاتی رخ دهد. بنابراین، راهکار باید از محدوده وسیع دمای عملیاتی -۴۰°C تا ۷۵°C پشتیبانی کند.

محافظت در برابر ESD/Surge و جداسازی مغناطیسی

با توجه به عدم قطعیت‌های مرتبط با برق و میدان مغناطیسی در زیرساخت‌های حیاتی بدون نگهدارنده، گیتوی مورد نیاز باید مجهز به محافظت ESD/surge و همچنین جداسازی مغناطیسی ۱/۵ KV باشد تا اختلالات احتمالی به حداقل برسد.

LED برنامه‌پذیر

LED برنامه‌پذیر به اپراتورها پیام‌های وضعیت سیستم را به صورت بصری ارائه می‌دهد. این LED دارای پیام‌های پیش‌فرض است، اما مهندسین حاضر در محل می‌توانند آن را برنامه‌ریزی کنند تا پیام‌های خاص تنظیم شوند.

امنیت سایبری
شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

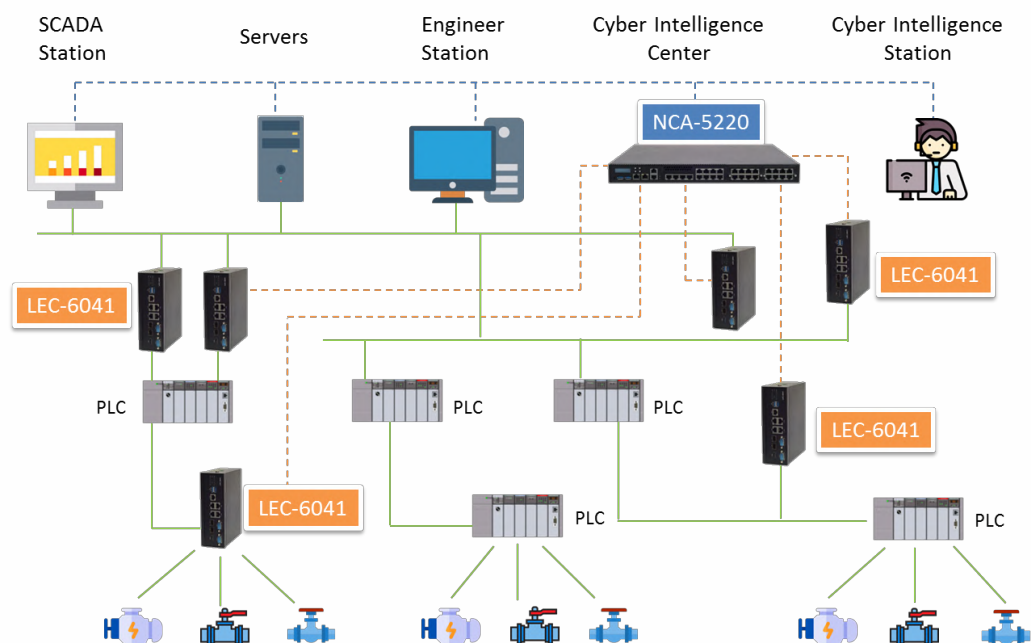
0933-6889690

www.navak-ai.ir

info@navak-ai.ir



IT/OT Industrial Cyber Security Deployment



امنیت سایبری

شبکه های کنترل صنعتی
 (OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



این مقاله توضیح می‌دهد که وقتی تجهیزات کنترل صنعتی مثل PLC، SCADA و HMI در شبکه‌های OT به هم متصل می‌شوند، گیتوی‌های زیادی برای حملات سایبری ایجاد می‌شود و باید با راهکارهای تخصصی امنیتی آن‌ها را محافظت کرد.

امنیت سیستم‌های کنترل صنعتی برای دارایی‌های حیاتی شما



پس از وقوع چندین حادثه بزرگ امنیت سایبری در زیرساخت‌های حیاتی، دولت‌ها و شرکت‌های بهره‌بردار از این امکانات، بدافزارها و باج‌افزارها را جدی گرفته‌اند. به‌وضوح، بدافزارها و باج‌افزارهایی مانند **WannaCry**، **Stuxnet** و **Crash Override** در چند سال اخیر، آسیب‌پذیری شبکه‌های SCADA و سیستم‌های کنترل صنعتی (ICS) در اتوماسیون شبکه برق، سیستم‌های ریلی، خطوط لوله گاز طبیعی، سایت‌های نفتی و سایر زیرساخت‌های حیاتی را آشکار کرده‌اند.

امنیت همگرای OT+IT

در محیط دیجیتالی متداول برای زیرساخت‌های حیاتی:

- **OT (فناوری عملیاتی)**، کنترل و مدیریت **Cell Zone** و **Area Zone** را برعهده دارد، مانند باس ابزار دقیق، LAN کنترلر و سیستم‌های HMI و SCADA نظارتی.
 - **IT (فناوری اطلاعات)**، نظارت و احراز هویت را بر بخش‌های **Enterprise** و **DMZ** مانند وب‌سرورها، سرورهای ایمیل، FTP و سرورهای سازمانی انجام می‌دهد.
- در یک مدل پیشرفته‌تر، یک **Industrial Zone** به‌عنوان لایه اضافی حفاظت در برابر سرویس‌های خارجی مستقر می‌شود.
- اوایل سال ۲۰۲۱، یک خط لوله حیاتی که برای سواحل شرقی آمریکا تأمین می‌کرد، پس از حمله گسترده باج‌افزاری به‌طور موقت تعطیل شد. چنین حوادث امنیت سایبری، تهدیدی روزافزون هستند و به‌ویژه برای زیرساخت‌های عمومی حیاتی، دولت‌ها را وادار به اجرای مقررات و دستورالعمل‌های جدید برای تقویت امنیت شبکه‌های صنعتی کرده‌اند.

دستگاه‌های امنیتی OT/IT

برای حفاظت از شبکه‌های ICS/OT، شرکت لَنر دستگاه‌های امنیتی شبکه‌ای مخصوص OT/IT ارائه می‌دهد که برای مدیریت، نظارت و کنترل سیستم‌های ICS و SCADA زیرساخت‌های حیاتی طراحی شده‌اند. این دستگاه‌ها قابلیت‌هایی مانند فیلترینگ پروتکل‌ها، بازرسی بسته‌ها، فهرست سفید و نظارت بر ترافیک شبکه را ارائه می‌کنند.

این رایانه‌های صنعتی از طریق ترکیبی از مهندسی مکانیکی و حرارتی طراحی شده‌اند تا مشکلاتی مانند نوسانات برق، در دسترس بودن بالا، دمای شدید و استانداردهای صنعتی را پوشش دهند.

امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



در این مقاله اشاره شده که یک Firewall تخصصی صنعتی به مدیران کمک می کند تا زون بندی شبکه و انتقال فقط ترافیک مجاز بین بخش های مختلف را کنترل کنند.

امنیت سایبری Zero Trust و Defense-in-Depth برای شبکه های همگرا IT/OT



دنیای IT (فناوری اطلاعات) و OT (فناوری عملیاتی) در حال همگرایی با یکدیگر هستند و در صورت پیاده سازی صحیح، می توانند به طور چشمگیری بهره وری را افزایش دهند، خطاها را کاهش دهند، هزینه ها را کم کنند و گردش کارها را بهبود بخشند. این همگرایی مزایای بزرگی برای صنایع تولیدی، شرکت های آب و برق و انرژی، حمل و نقل، خرده فروشی، پزشکی و ارتباطات به همراه دارد. با این حال، علاوه بر مزایا، این همگرایی OT را در معرض طیف گسترده و پیشرفته ای از تهدیدات سایبری قرار می دهد.

این آسیب پذیری ها تهدیدی رو به رشد برای زیرساخت های حیاتی و سایر سامانه های مهم محسوب می شوند، زیرا اختلال در عملیات و ایمنی می تواند خسارات جدی ایجاد کند و حتی به آسیب های اعتباری (Reputational Damage) منجر شود. چالش های متعددی برای ایمن سازی کامل محیط OT وجود دارد و پیش از اتخاذ تصمیم نهایی، باید رویکردها و معماری های مختلف امنیتی با دقت بررسی شوند. دو مورد از رایج ترین معماری های امنیتی مورد استفاده، رویکردهای Zero Trust و Defense-in-Depth هستند.

امنیت Zero Trust و Defense-in-Depth

امنیت Zero Trust یک رویکرد جامع است که نیازمند احراز هویت سخت گیرانه برای هر فرد و هر دستگاهی است که قصد دسترسی به منابع شبکه را دارد؛ چه این دسترسی از داخل شبکه باشد و چه از خارج از محدوده شبکه. رویکرد Defense-in-Depth شامل مجموعه ای از لایه های دفاعی است که برای حفاظت از داده ها و اطلاعات ارزشمند به کار گرفته می شوند. این رویکرد چندلایه با در نظر گرفتن افزونگی های هدفمند، امنیت کلی سیستم را افزایش می دهد، مسیرهای مختلف حمله را پوشش می دهد و در صورت شکست لایه اول، فرصت دوباره ای برای حفاظت از نواحی مختلف فراهم می کند.

با ترکیب این دو رویکرد، سازمان ها می توانند یک معماری امنیتی با چندین لایه حفاظتی به عنوان پایه ایجاد کرده و سپس با استفاده از مکانیزم های Zero Trust، کنترل دسترسی را در تمامی سطوح به صورت سخت گیرانه اعمال کنند.



ارتقای آگاهی امنیت سایبری

یکی دیگر از رویکردهای کلیدی، درک اهمیت ارتقای آگاهی و نگرش امنیت سایبری در تمامی سطوح سازمان است. همه اعضای تیم باید تشویق شوند تا علاوه بر رعایت الزامات فنی امنیت، مزایای آن را درک کنند. این موضوع شامل هماهنگی در واکنش‌های امنیتی، پایش و مدیریت شبکه، و اطمینان از وجود فرآیندهای قوی بازیابی و پاسخ به حوادث است؛ با این فرض ذهنی که همه دستگاه‌ها و شبکه‌ها می‌توانند مورد نفوذ قرار گیرند.

پیاده‌سازی احراز هویت قوی

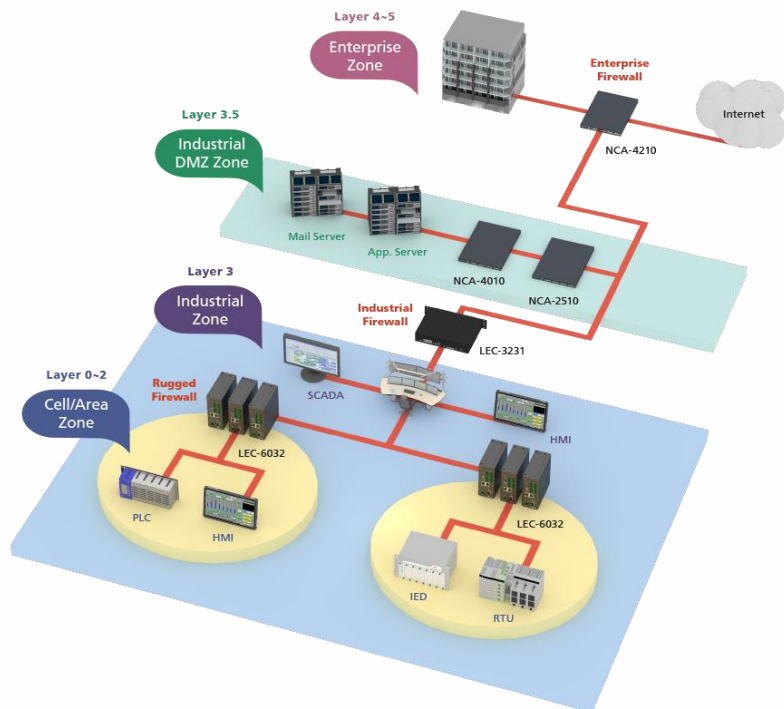
استفاده از احراز هویت قوی یکی دیگر از اقدامات حیاتی در شبکه‌هایی است که از معماری Zero Trust بهره می‌برند. این موضوع باید شامل کنترل دسترسی دستگاه‌ها، احراز هویت و مجوزدهی کاربران، و تعریف لیست‌های اعتماد برای آدرس‌های IP و پورت‌های سرویس باشد.

استفاده از بخش‌بندی شبکه (Network Segmentation)

بخش‌بندی مناسب شبکه می‌تواند از دسترسی تهدیدات ناشی از اتصال‌های راه دور و همچنین تهدیدات داخلی به کل شبکه جلوگیری کند. بخش‌بندی در سطح بالا، مانند استفاده از فایروال‌ها، مانع از حرکت جانبی تهدیدات مخرب در سراسر شبکه می‌شود.

فایروال‌ها به مدیران شبکه کمک می‌کنند تا نواحی (Zones) مختلفی را در شبکه تعریف کرده و فقط ترافیک مجاز را بین این نواحی عبور دهند. با افزودن سیاست‌ها و قوانین امنیتی، مانند محدودسازی آدرس‌های IP و مجاز دانستن تنها پورت‌های مورد استفاده، می‌توان شبکه را به بخش‌های کوچک‌تر و قابل‌مدیریت‌تر تقسیم کرد تا فقط ترافیک ضروری اجازه عبور داشته باشد.

مدل Zero Trust از ریزبخش‌بندی (Micro-Segmentation) پشتیبانی می‌کند که از طریق سیستم جلوگیری از نفوذ (IPS) پیاده‌سازی می‌شود. این رویکرد به شبکه امکان می‌دهد تهدیدات شناسایی‌شده را تشخیص داده و با محدود کردن حملات سایبری به نواحی مشخص، از دارایی‌های حیاتی محافظت کند. IPS به‌صورت مداوم رخدادهای مشکوک و مخرب را پایش می‌کند تا از گسترش حمله جلوگیری شده و امکان عیب‌یابی و بازیابی سریع شبکه فراهم شود.



امنیت سایبری

شبکه‌های کنترل صنعتی
(OT / SCADA)

ناوک هوشمند پویان

021-88109330

0933-6889690

www.navak-ai.ir

info@navak-ai.ir



LEC-6032C

Industrial Grade Cyber Security Appliance
with Intel® Atom™ E3845 Processor



■ Features

- Fanless industrial grade security appliance
- Intel® Atom™ E3845 1.91GHz SoC CPU
- Industrial security appliance with advanced Gen.3 bypass
- Wide operating temperature -40~75°C
- Flexible LAN: 5x GbE + 2x SFP ports
- Support dual power inputs

■ Preliminary Specifications

Processor System

CPU	Intel Atom E3845
Frequency	1.91 GHz
Core Number	4
BIOS	AMI SPI Flash BIOS
Chipset	N/A

Memory

Technology	DDR3L, 1333 MHz
Max. Capacity	8 GB
Socket	1 x 204-pin SODIMM

Graphic

Controller	Intel HD Graphics
VGA pin-header	1 x internal VGA pin-header

Ethernet

Controller	Intel i210-IT
Speed	10/100/1000 Mbps
Interface	5 x RJ45 & 2 SFP ports
LAN Bypass	1 pair
Magnetic Isolation Protection	1.5 KV built-in

Storage

Type	SATA
Installation	1x SATA connector, optional 2.5" drive bay

I/O

Serial Port	1 x DB9 RS232
ESD Protection	15KV ESD Protection
USB 3.0 / USB 2.0	1 x USB 3.0 / 1 x USB 2.0
Power-On/Reset Button	Internal reset button
LED	HDD, RUN, PWR, SFP

Watchdog Timer

Watchdog timer 256 level time interval system reset, software programmable

Power

Power Supply Voltage	12 ~ 36 Vdc, 6032E: 24 Vdc
Connector	Phoenix contact 6-pin connector w/ lock
Dual power inputs	Yes
Power Consumption (Idle)	9 ~ 10W
Power Consumption (Full Load)	15 ~ 16W
Power Adaptor	None

Environment

Operating Temperature	-40 ~ 75°C
Storage Temperature	-40 ~ 85°C
Relative Humidity	5% ~ 95%, non-condensing

Mechanical

Dimension (W x H x D)	78 x 146 x 127 mm
System Cooling	Fanless
Construction	Aluminum + SGCC
Weight	1 kg
Mounting	DIN rail or Wall mount

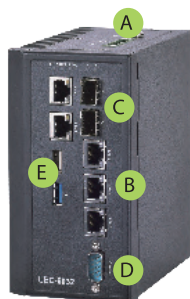
Driver Support

Microsoft Windows	Windows 7, Windows 7 Embedded
Linux	Kernal 3.X

Certification

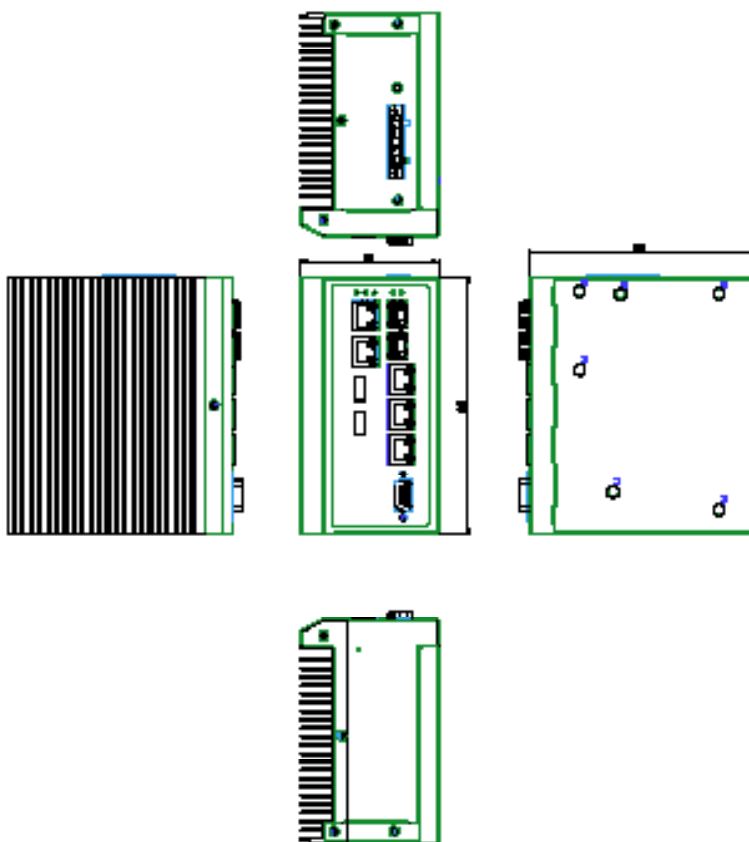
EMC	CE/FCC Class A
Safety	None

■ Product I/O View



- | | |
|-------------|-------------|
| A DC IN | D DB9 RS232 |
| B RJ45, GbE | E USB |
| C SFP | |

■ Dimensions (WxHxD): 78 x 146 x 127 mm



■ Ordering Information

LEC-6032C

Wide Temperature DIN rail Fanless Box PC with Intel Atom E3845 processor, 5 x GbE RJ45 with 1 pair Gen 3 bypass, 2 x GbE SFP, 1 x USB 3.0 host, 1 x USB 2.0 host, 1 x DB9 RS232

LEC-6032C

NCA-4220

1U 19" Rackmount Appliance Powered by Intel
Xeon® E/Core™/Pentium®/Celeron® Processors
(Codenamed Coffee Lake)



Images are for reference only. See ordering information for SKU details.

■ Features

- Intel® Xeon® E, Core™ i7/i5/i3, Pentium® or Celeron® CPU with C246/Q370/H310 Chipset
- 8x or 6x GbE RJ45 i210, 1x NIC Module
- 3x Pairs of Gen 3 LAN Bypass
- 2x 288-pin DIMM DDR4 2666MHz (Max. 32GB)
- 2x USB 3.0 Ports, 2x 2.5" HDD/SSD Intel Drive Bays (15 mm Height)
- 1x PCIe*8 FH/HL (Optional), 1x Mini-PCIe (PCIe/USB2.0)
- 3x or 2x Smart Fans (By SKU)

■ Specifications

Platform	
Form Factor	1U 19" Rackmount
Processor Options	Intel® Xeon® E, Core™ i7/i5/i3, Pentium® or Celeron® CPU (Coffee Lake)
CPU Socket	1x LGA1151
Chipset	Intel® C246/Q370/H310
Security Acceleration	N/A
BIOS	AMI SPI Flash BIOS
System Memory	
Technology	DDR4 up to 2666 UDIMM 8/16GB; ECC DIMM 8/16GB (SKU A Only)
Max. Capacity	32GB
Socket	2 x 288-pin DIMM
Networking	
Ethernet Ports	8 x or 6 x GbE RJ45 Intel® i210
Bypass	3 Pairs Gen3
NIC Module Slot	1
LOM	
IO Interface	N/A
OPMA Slot	N/A
I/O Interface	
Reset Button	1
LED	Power/Status/Storage
Power Button	1 x ATX Power Switch
Console	1 x RJ45
USB	2 x USB 3.0
LCD Module	2 x 20 Character LCM
	4 x Keypads
Display	From Mini-PCIe Slot (Optional)
Power Input	AC Power Inlet on PSU
Storage	

HDD/SSD Support	2 x 2.5" Intel Bays (15 mm Height)
Onboard Slots	1 x M.2 (SATA), 1 x M.2 (NVME)
Expansion	
PCIe	1x PCIe*8 FH/HL (Optional)
mini-PCIe	1x Mini-PCIe (PCIe/USB2.0)
Miscellaneous	
Watchdog	Yes
Internal RTC with Li Battery	Yes
TPM	Yes (Optional)
Cooling	
Processor	Passive CPU Heatsink
System	3 x or 2 x Cooling Fans with Smart Fan
Environmental Parameters	
Temperature	0~40°C Operating -20~70°C Non-Operating
Humidity (RH)	5~90% Operating 5~95% Non-Operating
System Dimensions	
(WxDxH)	438 x 321 x 44 mm
Weight	7.5 kg
Package Dimensions	
(WxDxH)	540 x 500 x 230 mm
Weight	8.5 kg
Power	
Type / Watts	220W ATX Single PSU
Input	AC 100~240V @50~60 Hz
Certication	
Approvals and Compliance	RoHS, CE/FCC Class A, UL

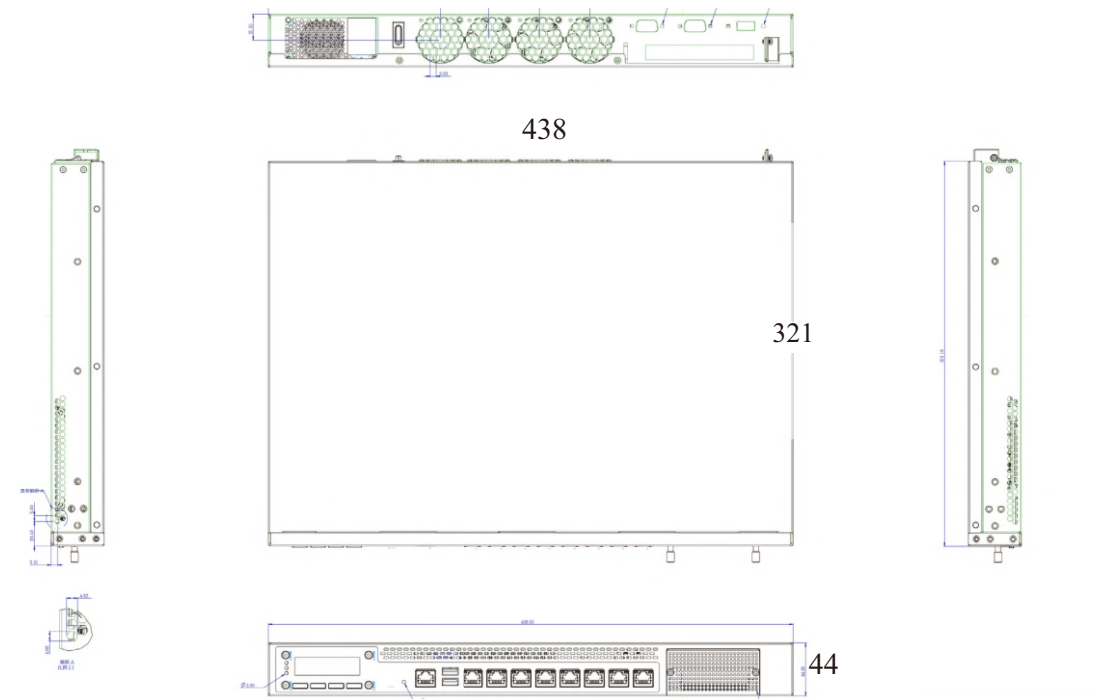
Product I/O View

Images are for reference only. See ordering information for SKU details.



- | | | |
|-----------------------|------------------------------|-----------------------|
| A LED | E USB 3.0 | I Cooling Fans |
| B LCM & Keys | F LAN Ports | J Power On/Off |
| C Reset Button | G NIC Slot | K PSU |
| D Console Port | H PCIe Slot (SKU A&B) | |

Dimensions (WxDxH) 438 x 321 x 44 mm



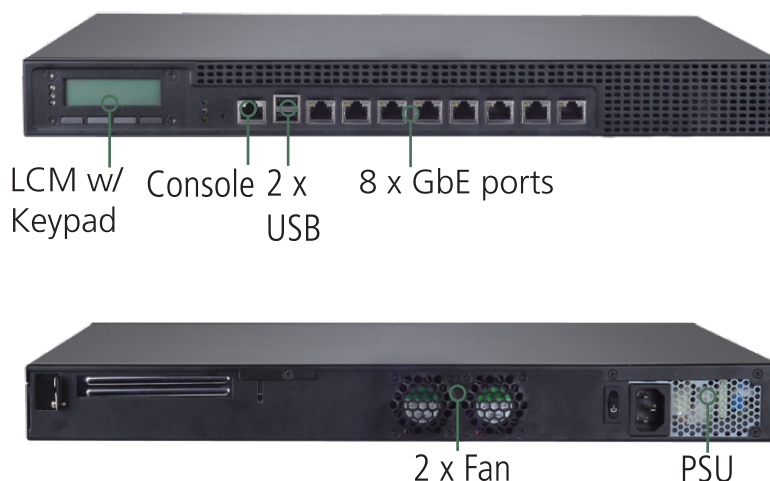
NCA-4220

Ordering Information

NCA-4220A	Intel Coffee Lake, Coffee Lake-S Processor, PCH C246, 2x DDR4 U-DIMM/ECC-DIMM (by CPU), 8x Gbe RJ45, with 3 Pairs of Bypass, 1x RJ45 Console 1x NIC Module Slots (1x PCIe*8 or 2x PCIe*4), 1x LCM, 1x 220W Single PSU
NCA-4220B	Intel Coffee Lake, Coffee Lake-S Processor, PCH Q370, 2x DDR4 U-DIMM (by CPU), 8x Gbe RJ45, with 3 Pairs of Bypass, 1x RJ45 Console 1x NIC Module Slots (1x PCIe*8 or 2x PCIe*4), 1x LCM, 1x 220W Single PSU
NCA-4220C	Intel Coffee Lake, Coffee Lake-S Processor, PCH H310, 2x DDR4 U-DIMM (by CPU), 6x Gbe RJ45, with 3 Pairs of Bypass, 1x RJ45 Console 1x NIC Module Slots (PCIEX8 only), 1x LCM, 1x 220W Single PSU

FW-7585

Rackmount x86 Network Security Platform Based on 4th Generation Intel® Core® i7/i5/i3 Series processor (Codenamed **Shark Bay)**



Features

4th Generation Intel® Core® processor i7/i5/i3 series with C226 (codenamed **Shark Bay)**

The 4th Generation Intel® Core® processor i7/i5/i3 series with C226 (codenamed **Shark Bay**) is a quad or dual-core processor featuring 22nm process technology with Tri-Gate transistors. Intel AES New Instruction (AES-NI), allow security algorithms to benefit from hardware acceleration for data encryption and decryption. The platform support dual-channel DDR3/DDR3L 1600 MHz memory at 1.5/1.35 V, thus it has power and space efficiency. The platform targeted at entry to mid branch office routers, security appliances, UTM or Next Generation Firewall appliances.

Intel® AES-NI Technology

With Intel new Haswell CPU, the FW-7585 can take full advantage of Intel® AES-NI technology to improve data encryption and decryption performance.

Watchdog Control LAN Bypass & Power Off LAN Bypass

The embedded watchdog monitors the system so that it can automatically trigger a reset if software hangs ; bypass ports allow users to have uninterrupted network traffic even if a single in-line appliance is shut down or is hung. Both are essential features of a network appliance. FW-7585 support 3 pairs of Generation 3 LAN Bypass.



Up to 7 Years Lifecycle Support

For Intel-based systems using chipsets and CPUs from Intel's embedded group we offer up to 7 years lifecycle support. This makes it possible for our customers to support their appliances for a longer time after deployment when compared to standard Intel server and desktop processors. Longer lifecycles can also be arranged by jointly planned inventories.

IPMI/Management port (By Project)

FW-7585 includes one IPMI/management port for in-band management and out-of-band remote management.

ECC Memory Support

FW-7585 supports Error-Correcting Code (ECC) memory technology, a servergrade memory technology that can identify and correct memory corruption automatically. With ECC, system performance is more secure and stable.

DDR3/L Low Voltage Memory Support

The FW-7585 supports DDR3L low voltage (1.35V) memory, it make whole system performance up to 5%~7% compare to previous generation CPU.

Dimensions (W x H x D): 431 x 44 x 305 mm

Preliminary Specifications

Form Factor		Rackmount
Platform	Processor Options	4th Generation Intel® Core™ processor i7/i5/i3 series with C226 (Codename Shark Bay)
	Chipset	C226
OS Support		Windows 7,8,2000, XP, Vista, Server 2008, 2012, Linux Kernel 2.6 or above
BIOS		AMI BIOS 64 Mb
System Memory	Technology	Dual-channel DDR3/DDR3L 1066/1333/1600 MHz, un-buffered, non-ECC
	Max. Capacity	16 GB
	Socket	2 x 240-pin DIMM
Storage	HDD Bays	2 x 2.5" HDD/SSD kit (reserved 1 x 3.5")
	CF/SD	1 x CF card Type II
Networking	Ethernet Ports	8 x GbE RJ-45 onboard
	Bypass	3 pairs Gen.3 (Optional)
	Controllers	1 x Intel i217, 7 x Intel i210AT
	Ethernet Modules	N/A
	Management Port	1 x GbE RJ-45
I/O Interface	Reset Button	1 x reset button
	Console	1 x RJ-45
	USB	2 x USB 2.0
	IPMI via OPMA slot	By Project
	Display	N/A
Expansion	PCIe	1 x PCIe x8 expansion at rear (Optional)
	PCI	N/A
Cooling	Processor	CPU heatsink
	System	2x cooling Fan with smart fan control
Environmental Parameters	Temperature, ambient operating / storage	0 ~ 40° C / -20~70° C
	Humidity (RH), ambient operating / ambient non-operating	5~90%, non-condensing / 5~95%, non-condensing
Miscellaneous	LCD Module	2 x 20 LCM with keypad
	Watchdog	Yes
	Internal RTC with Li Battery	Yes
Physical Dimensions	Dimensions (WxHxD)	431 x 44 x 305 mm
	Weight	7 kg
Power	Type / Watts	220 W / 150 W ATX Power Supply Units
	Input	AC 90~264 V @47~63 Hz
Approvals and Compliance		CE Class A, FCC Class A, RoHS



Ordering Information

FW-7585A

Rackmount x86 Network Security Platform Based on 4th Generation Intel® Core™ processor i7/i5/i3 series with C226 (Codenamed Shark Bay), 8 Intel GbE LAN ports with Gen.3 Bypass, 220 W / 150W ATX PSU



Feature	NHP-C10	NHP-C30	NHP-CR30	NHP-C50	NHP-CR50
Product Type	Industrial Firewall Appliance	Industrial Firewall Appliance	Rack Mount Appliance	Industrial Firewall Appliance	Rack Mount Appliance
Form Factor	Desktop model with DIN-rail mounting capability	Desktop model with DIN-rail mounting capability	1U Rackmount (Improved thermal design)	Industrial PC with IP67 Standard	1U Rackmount (Improved thermal design)
Enclosure / Build	Full metal industrial-grade chassis	Full metal industrial-grade chassis	Full metal industrial-grade chassis	Full metal chassis, reinforced for higher thermal load	Full metal industrial-grade chassis
Cooling Method	Passive (fanless)	Passive (optimized heatsink design)	Passive (optimized heatsink design)	Passive, next-gen thermal path for higher TDP	Passive (optimized heatsink design)
Dimensions	17.5 × 12.6 × 3.7 cm	17.5 × 12.6 × 3.7 cm	431 x 44 x 305 mm	78 × 146 × 127 mm	438 × 44 × 321 mm
Power Supply	12 V DC / 2 A (≈ 24 W max)	12 V DC / 2 A (≈ 24 W max)	220 W ATX PSU AC 90~264 V @47~63Hz	12~48 V DC / 3 A (≈ 40 W max, Dual Redundant)	220 W ATX PSU AC 90~264 V @47~63Hz
Operating Temp.	-10 °C ~ +60 °C	-10 °C ~ +60 °C	-5 °C ~ +40 °C	-40 °C ~ +75 °C	-5 ~ +40 °C
Storage Temp.	-20 °C ~ +50 °C	-20 °C ~ +50 °C	-20 °C ~ +50 °C	-40 °C ~ +80 °C	-20 °C ~ +50 °C
Humidity	5~90 % RH	5~90 % RH	5~90 % RH	5~90 % RH	5~90 % RH
Vibration / Shock	IEC 60068-2 compliant	IEC 60068-2 compliant	IEC 60068-2 compliant	IEC 60068-2 compliant	IEC 60068-2 compliant
Ethernet Ports	2 × RJ45 (1 GbE)	2 × RJ45 (1 GbE)	8 × GbE RJ-45 onboard 3 pairs Gen.3 1 × GbE RJ-45	5 × (10/100/1000 BaseT(X) / SFP+)	1x GbE RJ45, 8x 2.5GbE RJ45, 1x NIC Module 3x Pairs Of Gen 3 SE LAN Bypass
Serial Ports	2 × RS-232 (DB9)	2 × RS-232 (DB9)	1 × RS-232 (DB9)	Supported (RS-232/RS-485)	1 × RS-232 (DB9)
USB Ports	4 (2×USB2.0, 2×USB3.0)	4 (2×USB2.0, 2×USB3.0)	2 (2×USB2.0)	2 (1×USB2.0, 1×USB3.0)	2 × USB 3.0
Display Output	VGA, HDMI	VGA, HDMI	N/A	VGA, HDMI	VGA, HDMI (needs add on Module)
Console Access	Web/SSH/CLI + Serial Console	Web/SSH/CLI + Serial Console	Web/SSH/CLI + Serial Console	Web/SSH/CLI + Serial Console	Web/SSH/CLI + Serial Console
Network Standards	IEEE 802.3/ab/u/z/x, 802.1Q	IEEE 802.3/ab/u/z/x, 802.1Q	IEEE 802.3/ab/u/z/x, 802.1Q	IEEE 802.3/ab/u/z/x, 802.1Q	IEEE 802.3/ab/u/z/x, 802.1Q
Routing	VRRP Routing Redundancy	VRRP Routing Redundancy	VRRP Routing Redundancy	VRRP Routing Redundancy (enhanced stability)	VRRP Routing Redundancy
High Availability	Supported	Supported	Supported	Supported	Supported
VLAN Support	Up to 10 VLANs	Up to 50 VLANs	Up to 100 VLANs	Up to 100 VLANs	More than 100 VLANs
Throughput	Up to 100 Mbps (40 k PPS)	300 Mbps (70~90 k PPS)	500 Mbps (100~150 k PPS)	500 Mbps (80~150 k PPS)	800 Mbps (200~800 k PPS)
DPI Protocols	Modbus TCP/RTU, DNP3 , IEC-101/104, Ethernet/IP, Siemens S7,MQTT	Modbus TCP/RTU, DNP3 , IEC-101/104, Ethernet/IP, Siemens S7,MQTT	Modbus TCP/RTU, DNP3 , IEC-101/104, Ethernet/IP, Siemens S7,MQTT	Modbus TCP/RTU, DNP3 , IEC-101/104, Ethernet/IP, Siemens S7,MQTT	Modbus TCP/RTU, DNP3 , IEC-101/104, Ethernet/IP, Siemens S7,MQTT
DoS/DDoS Protection	Full DoS/DDoS Protection Suite	Full DoS/DDoS Protection Suite	Full DoS/DDoS Protection Suite	Full DoS/DDoS Protection Suite	Full DoS/DDoS Protection Suite
IPS / IDS	Advanced IPS/IDS (OT-aware)	Advanced IPS/IDS (OT-aware)	Advanced IPS/IDS (OT-aware)	Advanced IPS/IDS (OT-aware, higher capacity)	Advanced IPS/IDS (OT-aware, higher capacity)
VPN Type	IPsec VPN (≤5tunnels)	IPsec VPN (≤20 tunnels)	IPsec VPN (≤50 tunnels)	IPsec VPN (≤100 tunnels)	IPsec VPN (≤100 tunnels)
VPN Encryption	AES/3DES/DES	AES/3DES/DES	AES/3DES/DES	AES/3DES/DES	AES/3DES/DES
Authentication	SHA-256/MD5/RSA/X.509	SHA-256/MD5/RSA/X.509	SHA-256/MD5/RSA/X.509	SHA-256/MD5/RSA/X.509	SHA-256/MD5/RSA/X.509
VPN Throughput	80 Mbps	150 Mbps	250 Mbps	220 Mbps	300 Mbps
Firewall Modes	Router / Transparent	Router / Transparent	Router / Transparent	Router / Transparent	Router / Transparent
Management Protocols	HTTPS, SSH, SNMP v1/v2c/v3, CLI, Web GUI	HTTPS, SSH, IPsec, SNMP v1/v2c/v3, CLI, Web GUI	HTTPS, SSH, SNMP v1/v2c/v3, CLI, Web GUI	HTTPS, SSH, IPsec, SNMP v1/v2c/v3, CLI, Web GUI	HTTPS, SSH, SNMP v1/v2c/v3, CLI, Web GUI
Logging	Syslog, SNMP Trap, Local Storage	Syslog, SNMP Trap, Local Storage	Syslog, SNMP Trap, Local Storage	Syslog, SNMP Trap, Local Storage	Syslog, SNMP Trap, Local Storage
Applications	OT Segmentation, Remote Access, IDPS	Zone Isolation, Substation Cybersecurity	OT/IT Segmentation Remote Access Zone Isolation, Substation Cybersecurity VPN/IDPS	OT Segmentation, Remote Access Zone Isolation, Substation Cybersecurity	OT/IT Segmentation Remote Access Zone Isolation, Substation Cybersecurity VPN/IDPS

مشخصات مدل پایه NHP-C50

Input/Output Interface

Alarm Contact Channels	1 relay output with current carrying capacity of 1 A @ 24 VDC
Relay Channels	1

Ethernet Interface

Combo Ports (10/100/1000BaseT(X) or 100/1000BaseSFP+)	5
Standards	IEEE 802.1Q for VLAN Tagging IEEE 802.3 for 10BaseT IEEE 802.3ab for 1000BaseT(X) IEEE 802.3u for 100BaseT(X) and 100BaseFX IEEE 802.3x for flow control IEEE 802.3z for 1000BaseSX/LX/LHX/ZX

Ethernet Software Features

Management	Back Pressure Flow Control, DHCP, HTTPS, SMTP, SNMPv1/v2c/v3,
Routing	Throughput: 40,000 packets per second (max. 500 Mbps)
Routing Redundancy	VRRP
Security	HTTPS/SSL, SSH, IPsec
Time Management	NTP, SNTP

Switch Properties

Max. No. of VLANs	100
-------------------	-----

DoS and DDoS Protection

Technology	ARP-Flood, FIN Scan, ICMP-Death, NEWWithout-SYN Scan, NMAP-ID Scan, NMAPXmas Scan, Null Scan, SYN/FIN Scan, SYN/RST Scan, SYN-Flood, Xmas Scan
------------	--

Firewall

Deep Packet Inspection	Modbus TCP/RTU, Ethernet IP, DNP3, IEC104 /١٠١
Filter	DDoS, Ethernet protocols, ICMP, IP address, MAC address, Ports
Quick Automation Profiles	DNP, EtherCAT, EtherNet/IP, FOUNDATION Fieldbus, FTP, HTTP, IEC 60870-104, IPsec, L2TP, LonWorks, Modbus TCP, PPTP, PROFINET, RADIUS, SSH, Telnet
Stateful Inspection	Router firewall, Transparent (bridge) firewall
Throughput	Max. 80000 packets per second (max. 500 Mbps)

IPsec VPN

Authentication	MD5 and SHA (SHA-256) RSA (key size: 1024-bit, 2048-bit) X.509 v3 certificate
Concurrent VPN Tunnels	Max. 100 IPsec VPN tunnels
Encryption	3DES, AES-128, AES-192, AES-256, DES
Protocols	IPsec
Throughput	Max. 150 Mbps (Conditions: AES-256, SHA-256)

NAT

Features	1-to-1, N-to-1, Port forwarding
----------	---------------------------------

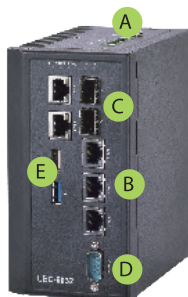
Real-Time Firewall / VPN Event Log

Event Type	Management log, System log, Security protection, Firewall, High Availability
Media	Local storage, SNMP Trap, Syslog server

Serial Interface

Console Port	Web /SSH/CLI, and RS-232 serial console
--------------	---

Dimensions (WxHxD): 78 x 146 x 127 mm



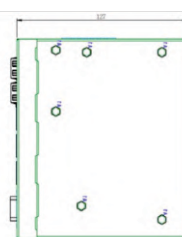
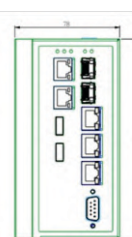
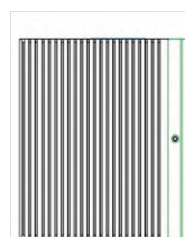
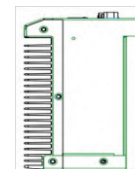
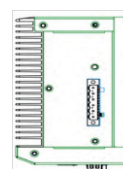
A DC IN

B RJ45, GbE

C SFP

D DB9 RS232

E USB



مشخصات مدل NHP-CR50



- | | | |
|----------------|-----------------------|----------------|
| A LED | E USB 3.0 | I Cooling Fans |
| B LCM & Keys | F LAN Ports | J Power On/Off |
| C Reset Button | G NIC Slot | K PSU |
| D Console Port | H PCIe Slot (SKU A&B) | |

Dimensions (WxDxH): 431 x 305 x 44 mm

مشخصات مدل NHP-CR30

