



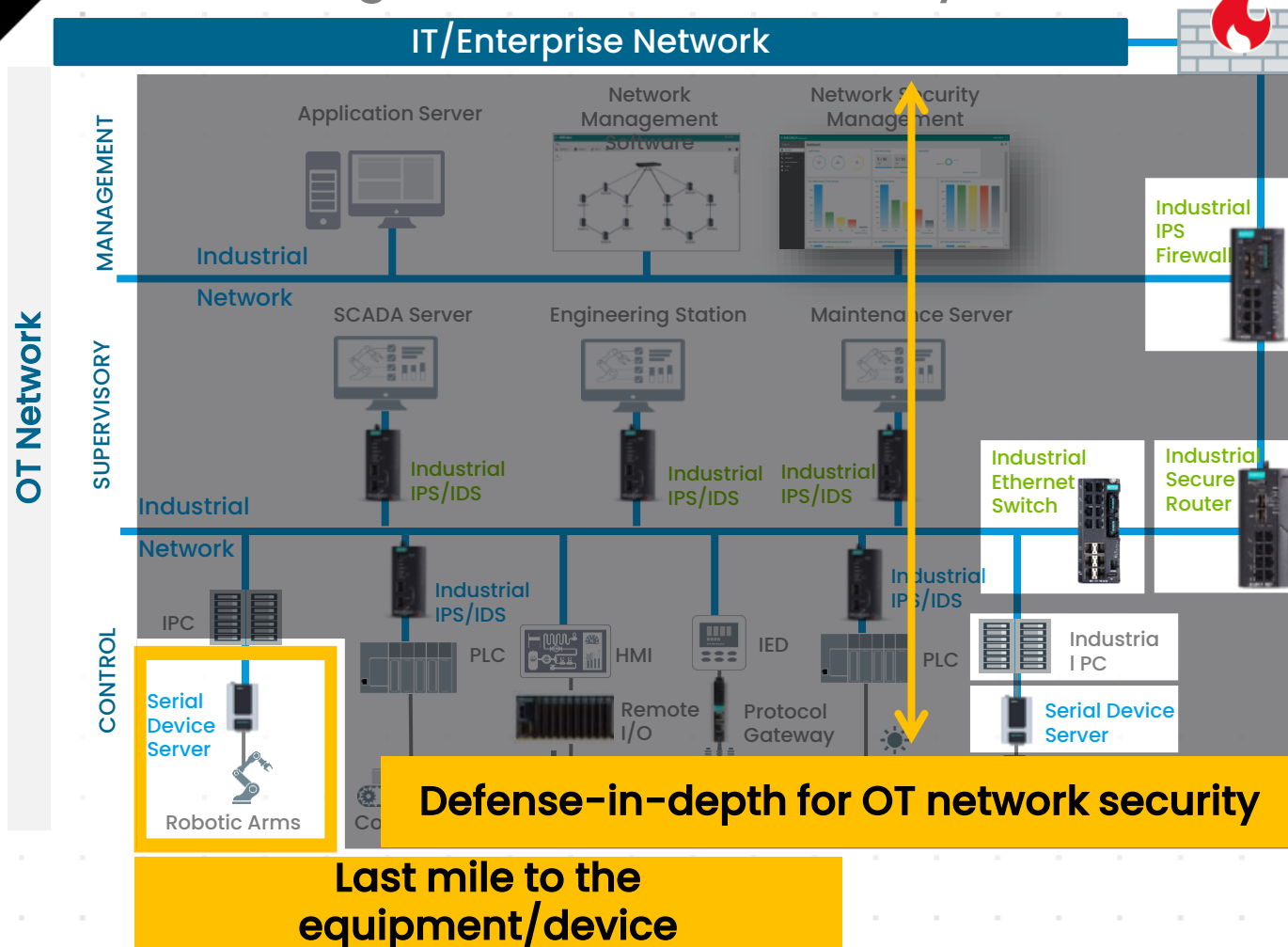
Elmark Automatyka

Nowa generacja komunikacji szeregowej –
bezpieczne rozwiązania i monitoring
w sieciach elektroenergetycznych

Dariusz Molenda

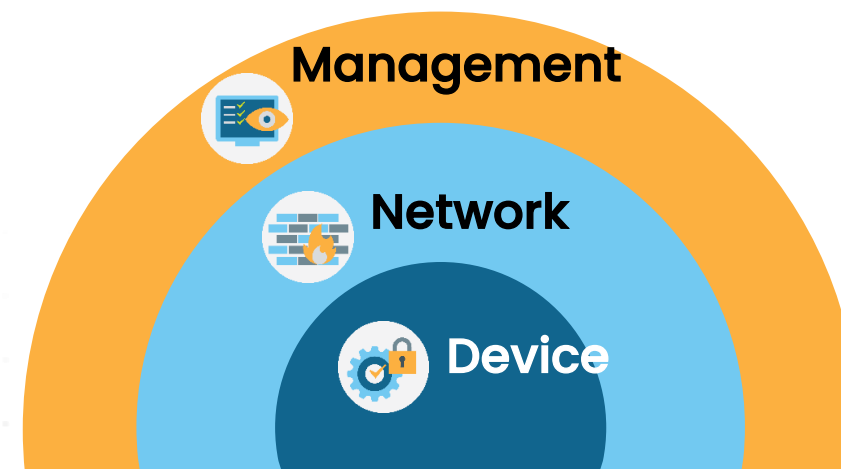
Dlaczego cyberbezpieczeństwa komunikacji szeregowej ma znaczenie?

OT-IT Integrated Network Security Solution



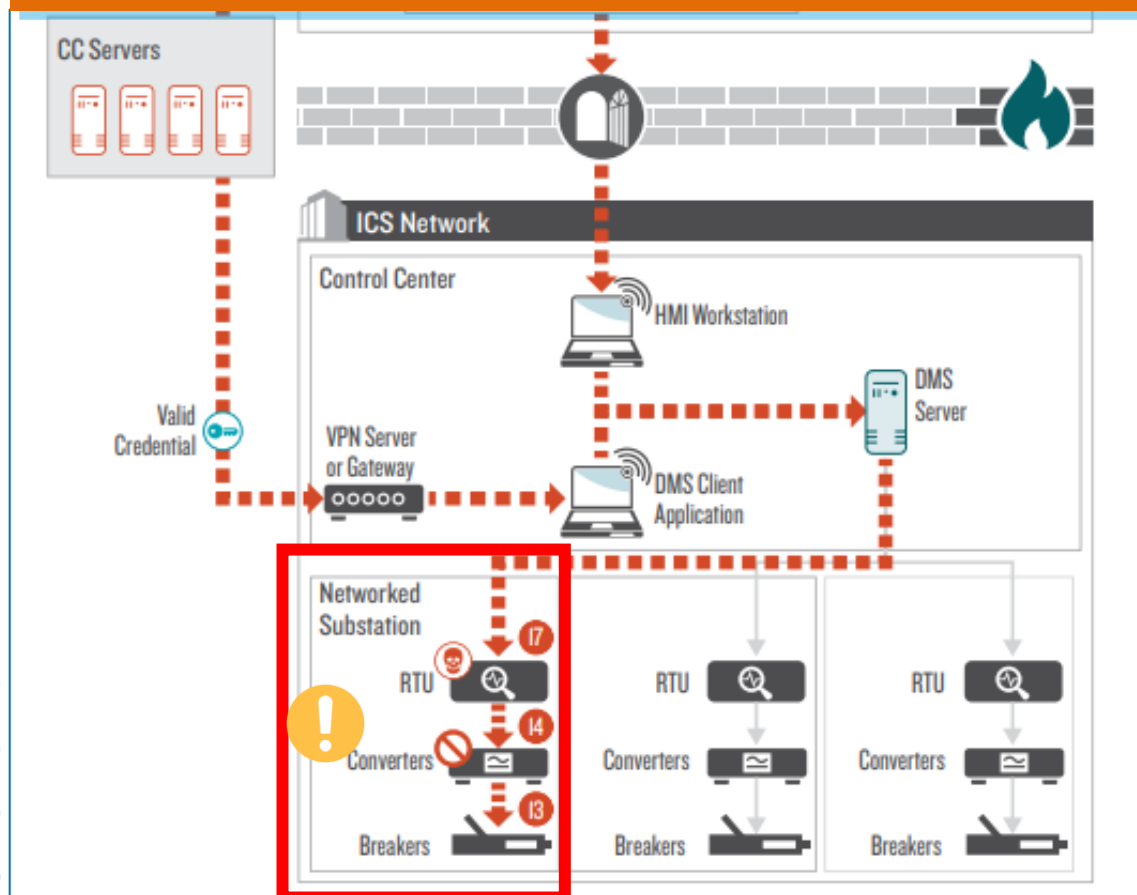
Holistic Security Strategy Aligned with IEC 62443

- Identify Network Status
- Protect Your Networks
- Select Secure Device



Dlaczego warto zadbać o cyberbezpieczeństwo komunikacji szeregowej?

Atak na sieć energetyczną na Ukrainie w 2015 r.



Fakty

Konwerter Serial-to-Ethernet był stosowany w celu podłączenia wyłączników do RTU jako połączenie zapasowe.

W ramach 17-etapowego ataku, jeden z kroków polegał na wyłączeniu konwertera, aby uniemożliwić odzyskanie kontroli przez połączenie zapasowe.

Rezultat

Ponad 230 000 osób doświadczyło przerwy w dostawie prądu trwającej od jednej do sześciu godzin.

Wnioski

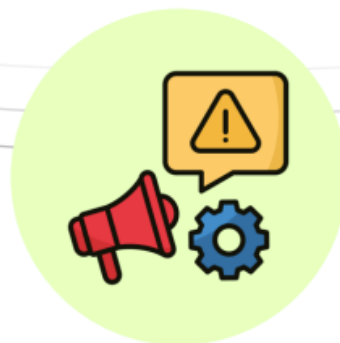
- Skuteczne cyberbezpieczeństwo wymaga **podejścia warstwowego (defense-in-depth)**.
- Podczas oceny zagrożeń należy **brać pod uwagę łączność brzegową (edge)** – np. urządzenia typu serwer portów szeregowych.

Dlaczego warto zadbać o cyberbezpieczeństwo komunikacji szeregowej?

Fakty i zagrożenia



Brak wbudowanych zabezpieczeń w urządzenia



Brak widoczności incydentów



Dane przesyłane są „czytelnie”, bez szyfrowania

28 lat, a mimo to wciąż zaangażowani w łączność szeregową



NPort



MGate



„Hej! Twoje urządzenie
OT musi być zgodne
z polityką
bezpieczeństwa firmy
bla bla bla...”



Musicie udowodnić, w
jaki sposób Wasza firma
chroni dane krytyczne
przed zagrożeniami
zgodnie z NIS2...

Bezpieczne połączenie szeregowo z siecią Ethernet kluczowe zagadnienia



Dostęp i integralność

Potencjalne zagrożenia:

- Niezamierzona błędna konfiguracja
- Wspólne domyślne hasło i brak poziomów uprawnień do urządzenia root
- Uruchamianie niezawerifikowanego oprogramowania



Bezpieczna komunikacja

Potencjalne zagrożenia:

- Wyciek danych procesowych w formie otwartego tekstu
- Niezabezpieczony interfejs zarządzania może umożliwić zmianę konfiguracji urządzenia
- Złośliwe działania w celu monitorowania lub przejęcia kontroli nad urządzeniem polowym



Rejestrowanie incydentów

Potencjalne zagrożenia:

- Brak widoczności raportów o incydentach i brak reakcji na zagrożenia
- Niedobór logów lub niewystarczające informacje o incydentach
- Konieczność zgodności z politykami audytu bezpieczeństwa (np. NIS2)



Polityka zarządzania

Potencjalne zagrożenia:

- Luki w produktach i bibliotekach open-source są stale wykorzystywane i odkrywane
- Ujawnienie danych logowania do urządzenia – konieczność okresowych aktualizacji

Jak zabezpieczyć?

Bezpieczne połączenie szeregowe z siecią Ethernet kluczowe zagadnienia



Dostęp i integralność

Potencjalne zagrożenia:

- Niezamierzona błędna konfiguracja
- Wspólne domyślne hasło i brak poziomów uprawnień do urządzenia root
- Uruchamianie niezwyfikowanego oprogramowania



Bezpieczna komunikacja

Potencjalne zagrożenia:

- Wyciek danych produkcyjnych w formie otwartego tekstu
- Niezabezpieczony interfejs zarządzania może umożliwić zmianę konfiguracji urządzenia
- Złośliwe działania w celu monitorowania lub przejęcia kontroli nad urządzeniem polowym



Rejestrowanie incydentów

Potencjalne zagrożenia:

- Brak widoczności raportów o incydentach i brak reakcji na zagrożenia
- Niedobór logów lub niewystarczające informacje o incydentach
- Konieczność zgodności z politykami audytu bezpieczeństwa (np. NIS2)



Polityka zarządzania

Potencjalne zagrożenia:

- Luki w produktach i bibliotekach open-source są stale wykorzystywane i odkrywane
- Ujawnienie danych logowania do urządzenia – konieczność okresowych aktualizacji

Jak zabezpieczyć?

- **Secure Boot (bezpieczny rozruch)** jest niezbędny dla zachowania integralności
- Uwierzytelnianie oparte na rolach użytkowników i kontrola dostępu do sieci
- Projektowanie pierwszego logowania tak, by wymuszać zmianę domyślnych loginów/hasła

Jak zabezpieczyć?

- Zabezpieczony strumień danych szeregowych i interfejs zarządzania z uwierzytelnieniem i szyfrowaniem
- Zaawansowane, odporne metody szyfrowania

Jak zabezpieczyć?

- Syslog z dokładnymi typami zdarzeń, poziomami zagrożeń i czasem
- Obsługa centralnych Syslogów dla integracji z systemami SoC/SIEM
- Unikanie nadpisywania lokalnej pamięci

Jak zabezpieczyć?

- Ciągłe zaangażowanie w aktualizowanie i łatki bezpieczeństwa ma kluczowe znaczenie
- Polityka haseł, która wymusza ich okresowe aktualizacje

Serwery portów szeregowych nowej generacji czyli NPort 6000-G2



NPort
Generation 2

Longevity / Easy Integration / Cyber Security

Nowe seria urządzeń NPort 6150-G2 / NPort 6250-G2



1. Opracowano zgodnie z procesem bezpiecznego projektowania

- Zespół certyfikowany zgodnie z normą IEC 62443-4-1
- Cykl życia produktu/projektowanie zgodnie z normami IEC 62443/CRA
- Zgodność z normą IEC 62443-4-2 Secure Level 2 (certyfikacja w planie*)

2. Zarządzenie cyberbezpieczeństwem

- Sprzętowa funkcja Secure Boot pozwala uruchamiać tylko zaufany firmware i konfigurację
- Uwierzytelnianie użytkowników przy użyciu kontroli dostępu opartej na rolach
- Proces pierwszego logowania bez domyślnej nazwy użytkownika i hasła
- Syslog do audytu incydentów

3. Bezpieczna komunikacja

- Zabezpieczony strumień danych szeregowych i interfejs zarządzania z szyfrowaniem i dodatkowym uwierzytelnianiem
- Obsługa najnowocześniejszej metody szyfrowania do RSA 4096 (lub ECC 521= RSA 15360)

4. Integracja w ramach systemu przedsiębiorstwa

- Obsługa zdalnego syslog (RFC3164) dla SIEM
- Obsługa zdalnego serwera uwierzytelniania dla serwera RADIUS/TACACS+

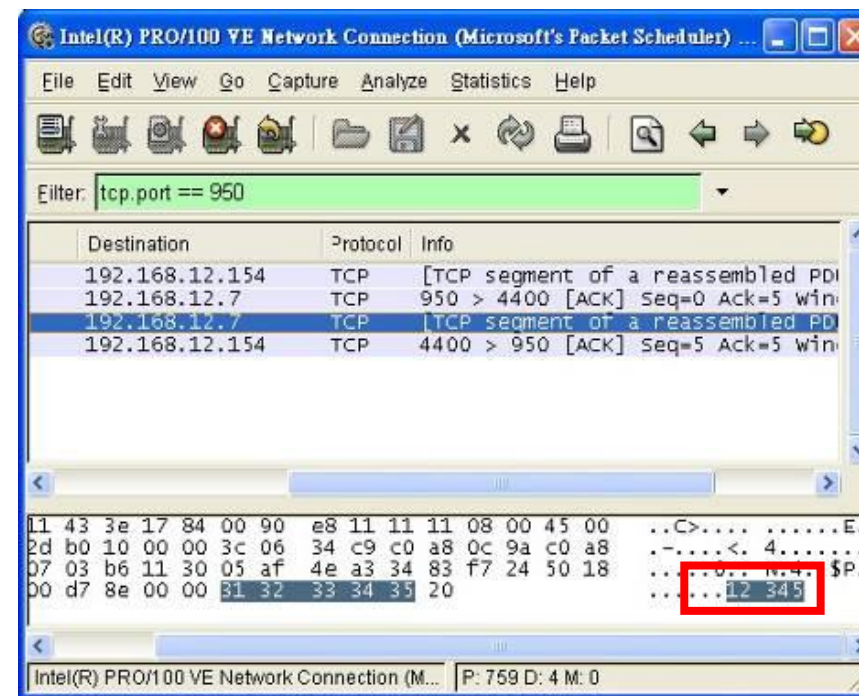
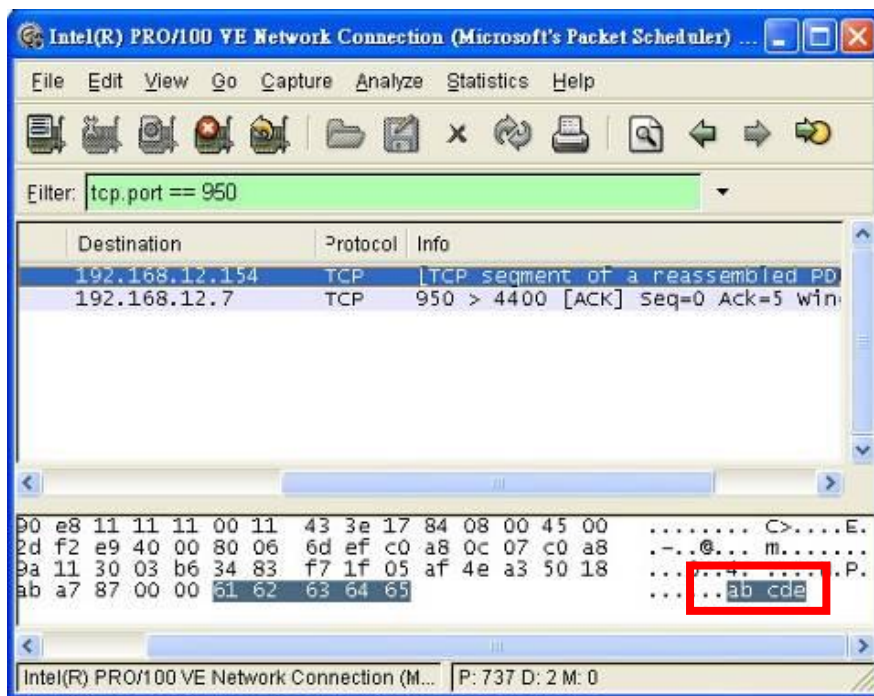
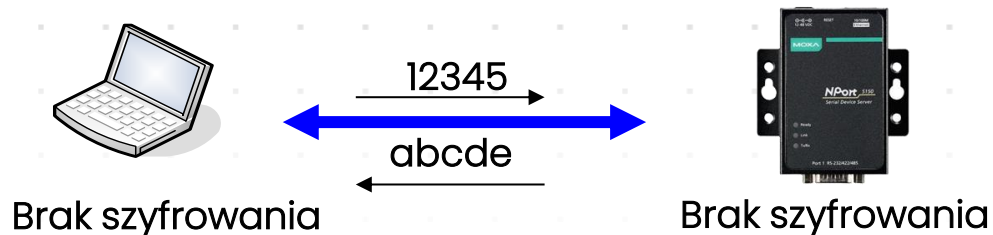
5. Ciągłość obsługi

- Ciągłe zaangażowanie w usuwanie i łatanie luk w zabezpieczeniach.

Model Selection	Serial Port	Secure Boot	SD Card for Serial Buffer	Operating Temperature
NPort 6150-G2	1	v	-	-10 to 60°C
NPort 6150-G2-T	1	v	-	-40 to 75°C
NPort 6250-G2	2	v	v	-10 to 60°C
NPort 6250-G2-T	2	v	v	-40 to 75°C

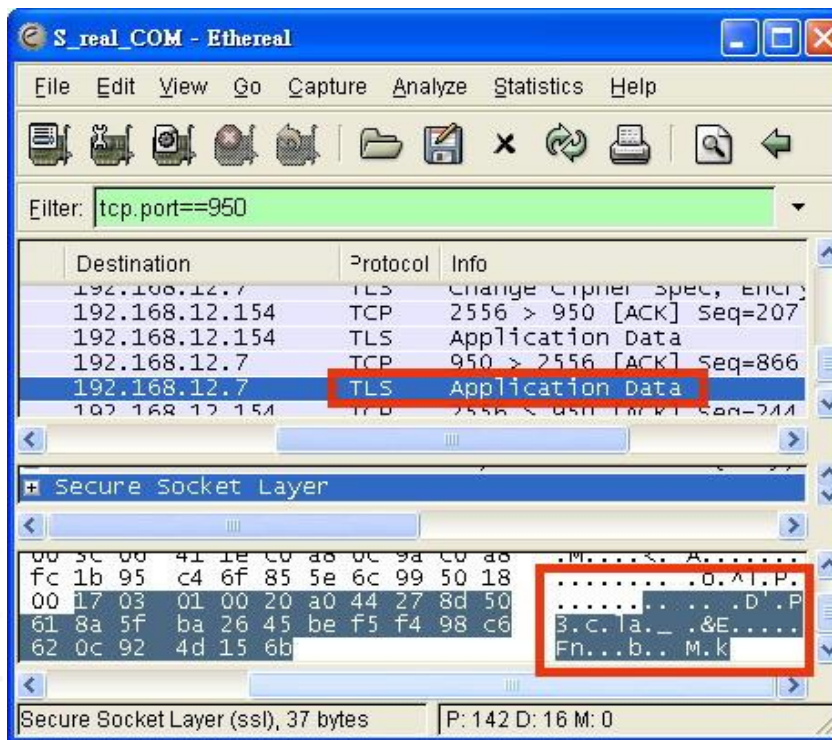
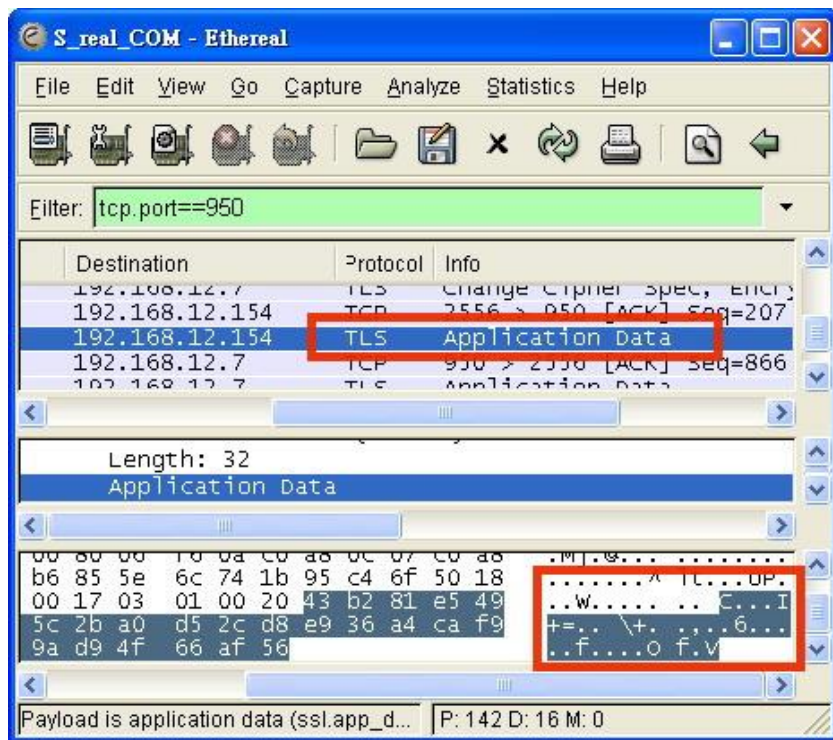
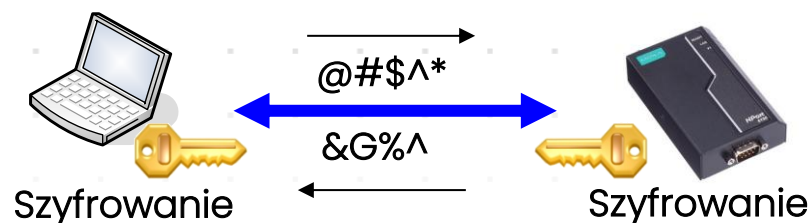
*plan certyfikacji koniec 2025 razem z wprowadzeniem modeli 4-32 portowych

Szyfrowanie transmisji w warstwie Ethernet



W normalnym trybie NPort 5000 nie szyfruje transmisji. Dane mogą być podsłuchane np. Wiresharkiem.

Szyfrowanie transmisji w warstwie Ethernet



Szyfrowanie transmisji – bezpieczniejsze algorytmy, uwierzytelnianie za pomocą certyfikatu SSL (*.pem)

Nowa konsola www



MOXA

Dashboard

System Settings

Network Settings

Serial Port Settings

Security

Account Management

Maintenance

Diagnostics

NPort 6250-G2

Administrator admin

Home > Dashboard

Dashboard

Device Information



Model Name

NPort 6250-G2

Device Name

NPort-6250-G2_3215

Description

--

Serial Number

TBD GB1043215

MAC Address

00:90:E8:C9:8C:DA

Firmware Version

v1.0.0 Build 24092704

System Operations

Time

System Time

2025-02-07T13:21:20

Uptime

0 day 01h:45m:14s

System State

CPU Usage

26%

Memory Usage

11%

Power Input1

Power on

SD Card

Undetected

Network Operations

Device Address

IPv4 Address

192.168.127.254

IPv6 Address

::

Running State

LAN1

100MB FD

System Log

Top 5 critical events within the past 30 days

VIEW MORE

Severity	Category	Event Name	Timestamp
Error	Security	Authentication fail	2025-02-07 12:46:22
Error	Security	Authentication fail	2025-02-07 12:46:21
Warning	Security	Account lockout	2025-02-07 12:46:20
Error	Security	Authentication fail	2025-02-07 12:46:20
Error	Security	Authentication fail	2025-02-07 12:46:19

Operation Mode State

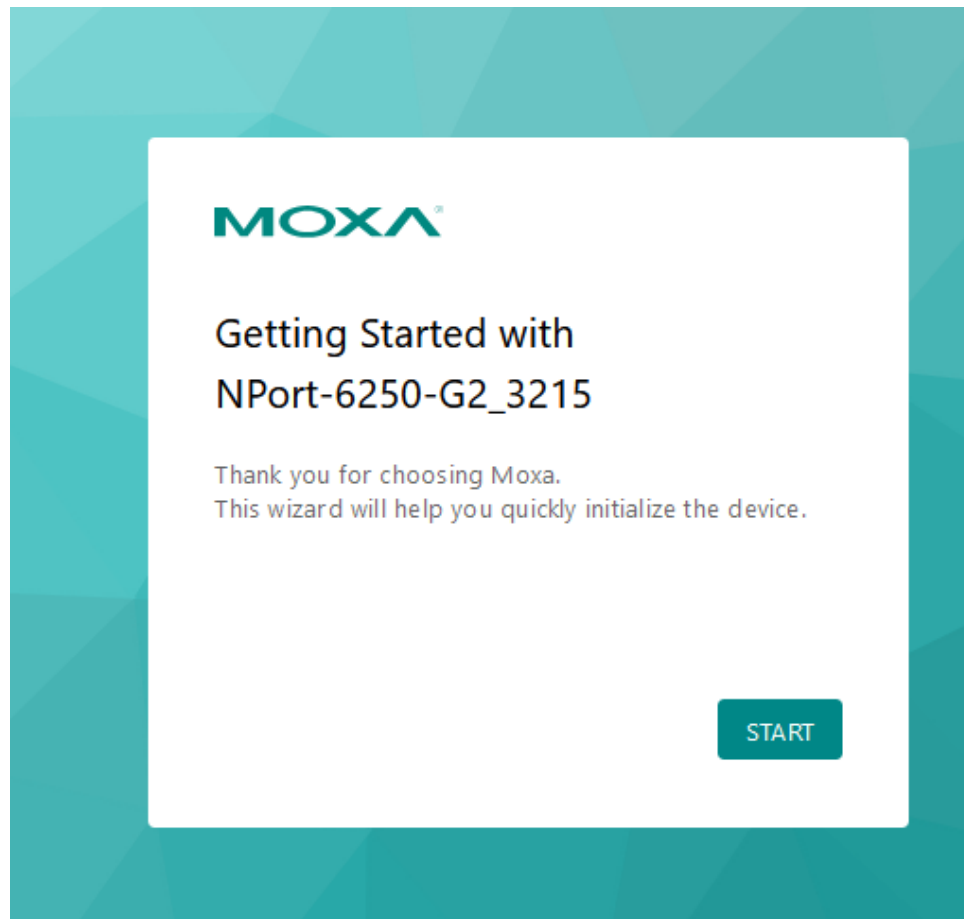
VIEW MORE

Port	Operation Mode	Connection Status	Serial Parameters	Serial Errors (count)
1	Real COM	Disconnected	RS-232, 19200, None, 8, 1	0
2	Real COM	Disconnected	RS-232, 0, None, 8, 1	0

Pierwsze uruchomienie



- ❑ Wizard który pozwala na przeprowadzenie konfiguracji krok po kroku



MOXA®

- 1 Import Configuration
Optional
- ✓ IP Settings
- 3 Create Account
- 4 Confirmation

Create Account

Create the first account of the device.

Account Name
admin

Password
••••••••



Confirm Password
••••••••



< BACK

NEXT >

Pierwsze uruchomienie



- ☐ Możliwość importu konfiguracji z serii NPort 6000 (1. generacja)



1 Import Configuration
Optional

2 IP Settings

3 Create Account

4 Confirmation

Import Configuration

Select the configuration file type to import, or skip this step.

File Type

-- Select One --

SKIP

NEXT >

Intuicyjna konfiguracja trybów pracy: wybór trybu

MOXA

Dashboard

System Settings

Network Settings

Serial Port Settings

- Operation Modes
- Serial Parameters
- Secure Connection

Security

Account Management

Maintenance

Diagnostics

NPort 6250-G2

Home > Serial Port Settings > Operation Modes > Configure Port(s)

← Configure Port(s)

1 Mode Selection

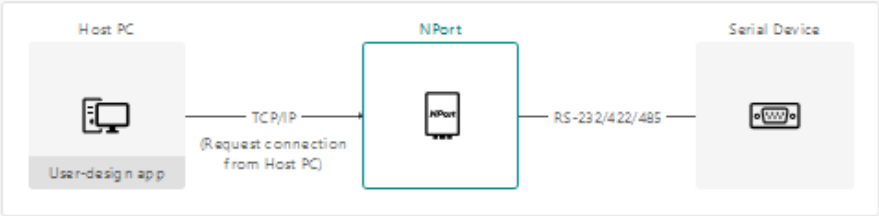
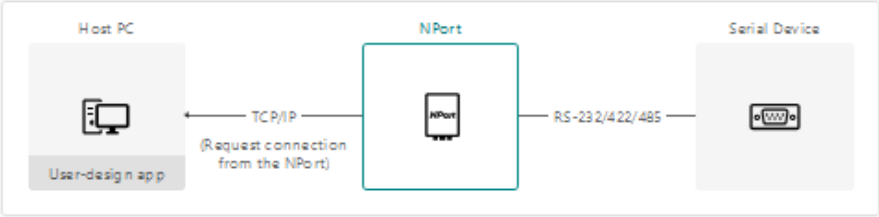
2 Basic Settings

First, select the application, then choose the operation mode that suits your needs.

Application

- Socket

Operation Mode

- ☒ TCP Server
 - The user's application establishes a TCP connection to the NPort, providing access to connected serial devices.

- ☐ TCP Client
 - The user's application listens to TCP connections from the NPort, providing access to connected serial devices.


Szczegółowe logi



MOXA

Dashboard

System Settings

Network Settings

Serial Port Settings

Security

Account Management

Maintenance

Diagnostics

NPort 6250-G2

Home > Diagnostics > System Log > Events Settings

← Events Settings

Select the events you would like to save in the system log. The events can be sorted by severity.
[Refer to the details of the severity](#)

Severity:

Error

Warning

Notice

Informational

System (16)

Network (7)

Security (23)

Maintenance (8)

Serial (8)

☐ Event Name	Severity
☒ Firmware ready	Notice
☐ Detect SD card	Informational
☒ SD card removed	Warning
☒ No SD card inserted	Error
☒ User trigger reboot	Notice
☐ Configuration changed	Informational
☒ Configuration changed failed	Notice
☐ NTP success	Informational
☒ NTP fail	Warning
☐ Manual setting time success	Informational
☒ Email fail	Notice
☒ SNMP inform fail	Notice

Szczegółowe logi



Dashboard

> System Settings

> Network Settings

> Serial Port Settings

> Security

> Account Management

> Maintenance

> Diagnostics

- Support
- System Log
- Operation Mode Statistics
- Network Monitor
- Ping
- Traffic Monitor

Home > Diagnostics > System Log

System Log

Log ViewLog Settings

FILTERCLEAREXPORTREFRESH

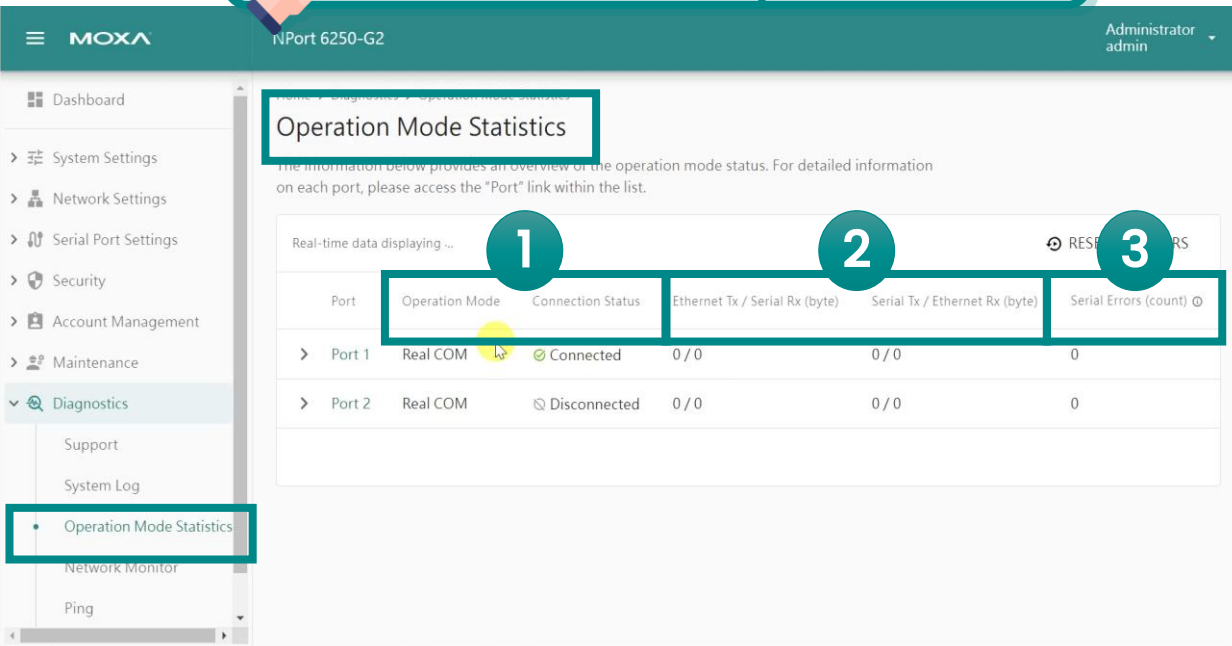
No	Severity	Category	Event Name	Timestamp
> 1	Informational	Security	Login success	2024-09-16 15:02:51
> 2	Informational	Security	Login success	2024-09-16 11:23:59
> 3	Informational	Security	Login success	2024-09-12 10:12:59
> 4	Informational	Security	Login success	2024-09-12 10:01:57
> 5	Error	Security	Authentication fail	2024-09-12 10:01:57
> 6	Notice	Serial	Port disconnect	2024-09-11 17:35:05
> 7	Notice	Serial	Port restart	2024-09-11 17:35:05

Items per page: 101 - 10 of 3911 / 40

Stan pracy portu szeregowego

1. Tryb pracy / status połączenia
2. Liczniki danych (Tx/Rx count) dla interfejsu Ethernet i interfejsu szeregowego
3. Licznik błędnych ramek interfejsu szeregowego

Szybkie sprawdzenie transmisji



Operation Mode Statistics

The information below provides an overview of the operation mode status. For detailed information on each port, please access the "Port" link within the list.

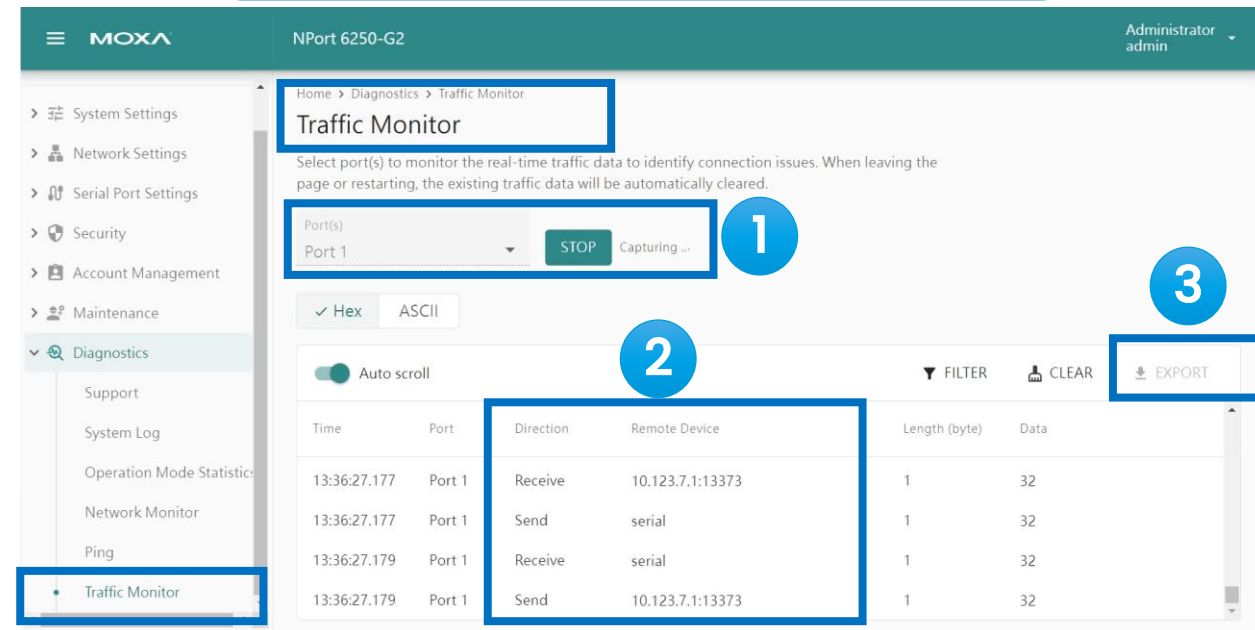
Port	Operation Mode	Connection Status	Ethernet Tx / Serial Rx (byte)	Serial Tx / Ethernet Rx (byte)	Serial Errors (count)
Port 1	Real COM	Connected	0 / 0	0 / 0	0
Port 2	Real COM	Disconnected	0 / 0	0 / 0	0

Real-time Traffic Monitoring

NEW

1. Wybierz port do monitorowania
2. Pakiety serial / Ethernet
3. Możliwość eksportu

Rozwiązywanie problemów



Traffic Monitor

Select port(s) to monitor the real-time traffic data to identify connection issues. When leaving the page or restarting, the existing traffic data will be automatically cleared.

Port(s): Port 1 STOP Capturing ...

Hex ASCII

Auto scroll

Time	Port	Direction	Remote Device	Length (byte)	Data
13:36:27.177	Port 1	Receive	10.123.7.1:13373	1	32
13:36:27.177	Port 1	Send	serial	1	32
13:36:27.179	Port 1	Receive	serial	1	32
13:36:27.179	Port 1	Send	10.123.7.1:13373	1	32

Online Traffic Monitor



Home > Diagnostics > Traffic Monitor

Traffic Monitor

Select the port(s) to be monitored for real-time traffic data, enabling the detection of connection problems. The existing traffic data will be cleared automatically when leaving or restarting the page.

Port(s)

Port 1

START

✓ Hex

ASCII

☒ Auto scroll

Time	Port	Direction	Remote Device	Length (Byte)	Data
14:32:29.968	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:29.995	Port 1	Receive	serial	9	01 04 04 01 22 00 ae db ce
14:32:29.996	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ae db ce
14:32:39.975	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:39.975	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:40.002	Port 1	Receive	serial	9	01 04 04 01 22 00 ae db ce
14:32:40.002	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ae db ce
14:32:50.004	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:50.004	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:32:50.032	Port 1	Receive	serial	9	01 04 04 01 21 00 ae 2b ce
14:32:50.032	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 21 00 ae 2b ce
14:32:59.988	Port 1	Receive	192.168.127.22:9769	8	01 04 00 01 00 02 20 0b
14:32:59.988	Port 1	Send	serial	8	01 04 00 01 00 02 20 0b
14:33:00.016	Port 1	Receive	serial	9	01 04 04 01 22 00 ad 9b cf
14:33:00.017	Port 1	Send	192.168.127.22:9769	9	01 04 04 01 22 00 ad 9b cf

Rezystory terminujące oraz pull high/low włączane/wyłączane z poziomu konsoli www

Configure Port(s)

Baudrate (bps)

9600

Parity

None

Data Bits

8

Stop Bit(s)

1

Flow Control

None

Advanced Settings

☒ Enable FIFO

Enabling FIFO results in increased throughput for serial communication. Disabling FIFO reduces latency.

☒ Enable terminator (120 Ω)

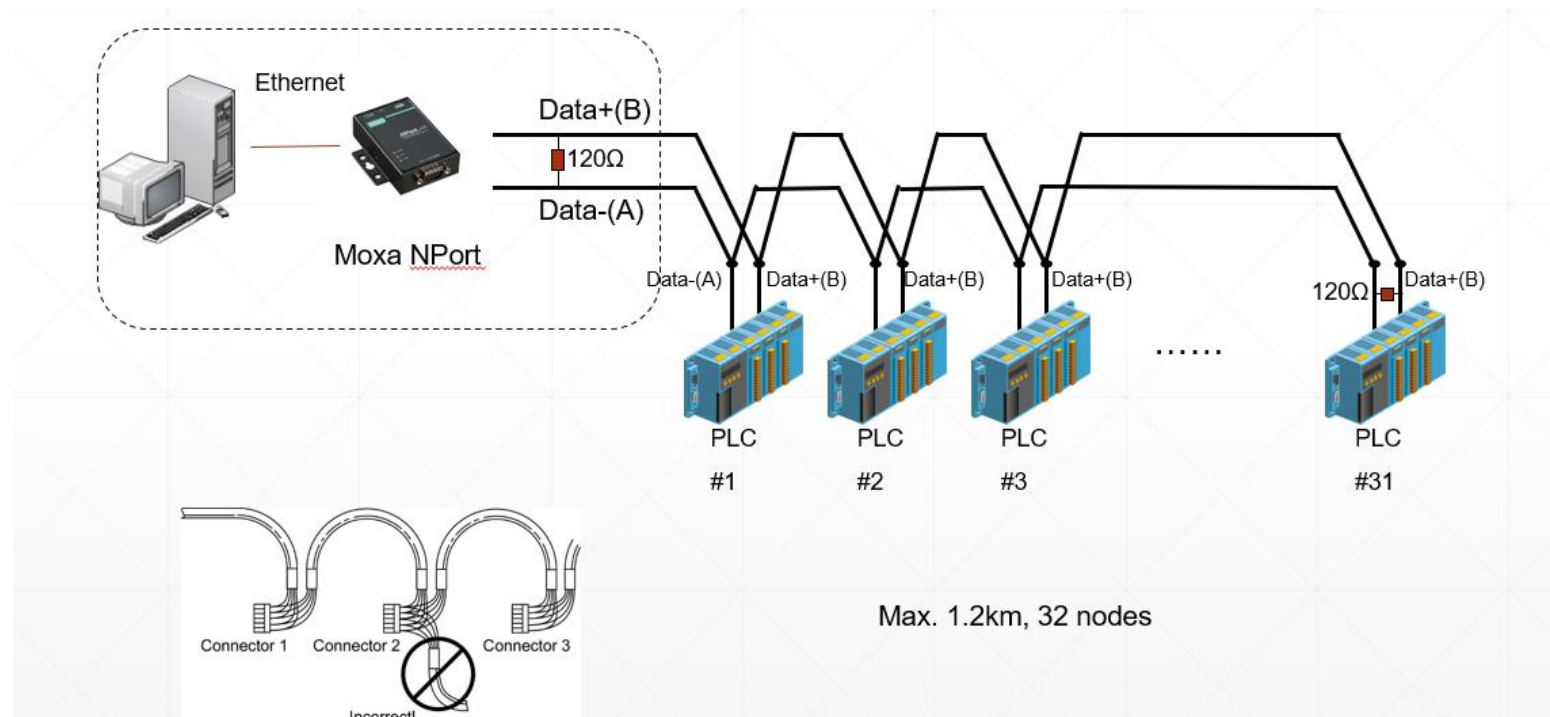
For RS-422/485, especially for long distance communication, we recommend you enable the terminator to prevent the reflection of serial signals on the first and the last RS-422/485 devices.

Resistor ⓘ

150 K Ω

CANCEL

SAVE

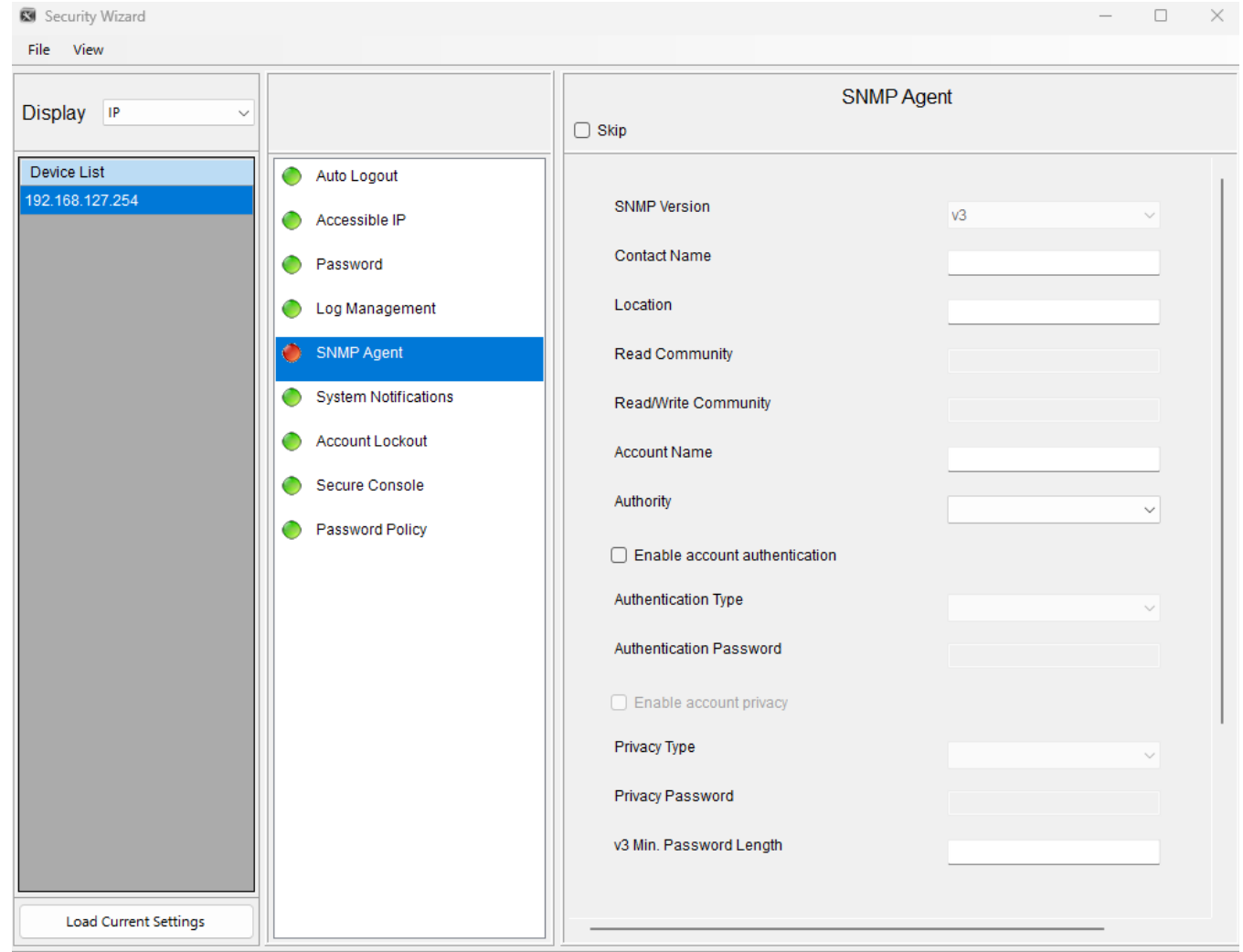


☐ Security Wizard w oprogramowaniu MXConfigCS

- ☐ łatwa implementacja zasad cyberbezpieczeństwa zgodnych z IEC 62443-4-2

☐ Security View w oprogramowaniu MxView One

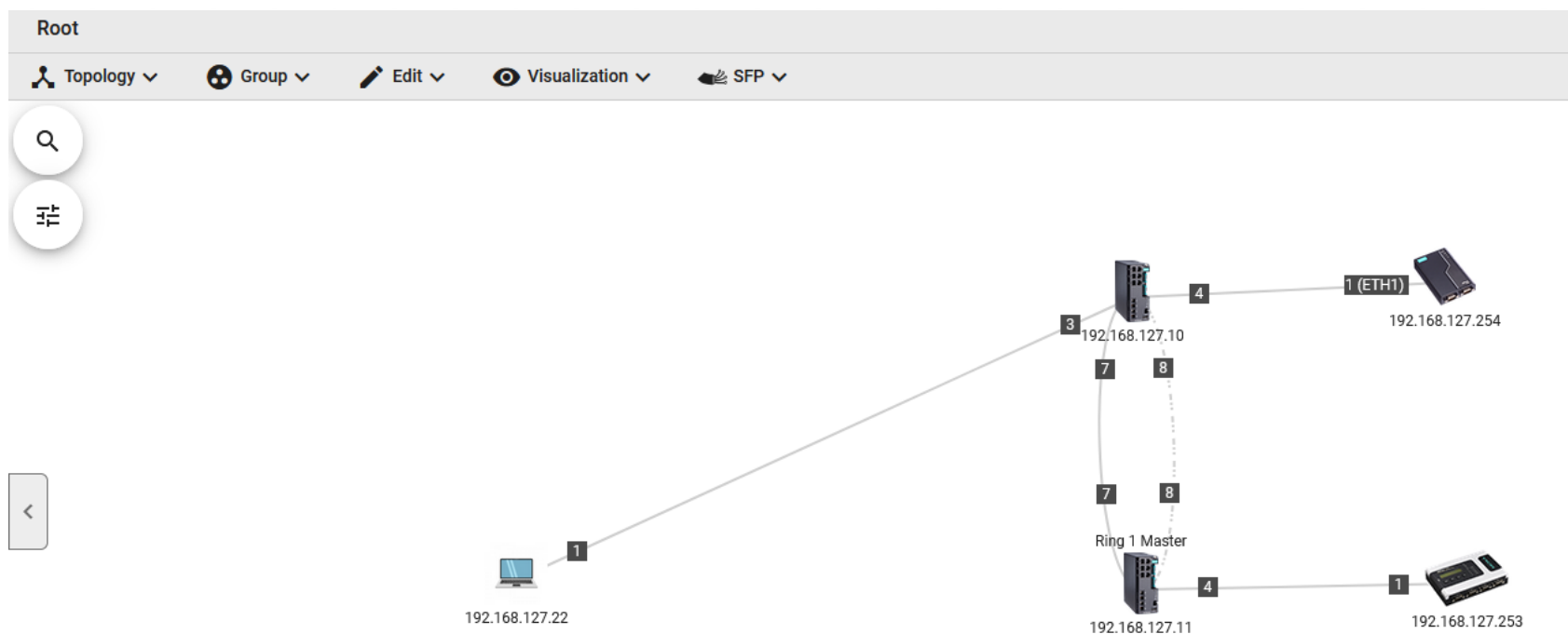
- ☐ audyt cyberbezpieczeństwa zgodnie z IEC 62443-4-2



The screenshot shows the 'Security Wizard' application window. The 'Device List' on the left contains the IP address '192.168.127.254'. The 'SNMP Agent' configuration panel on the right includes the following settings:

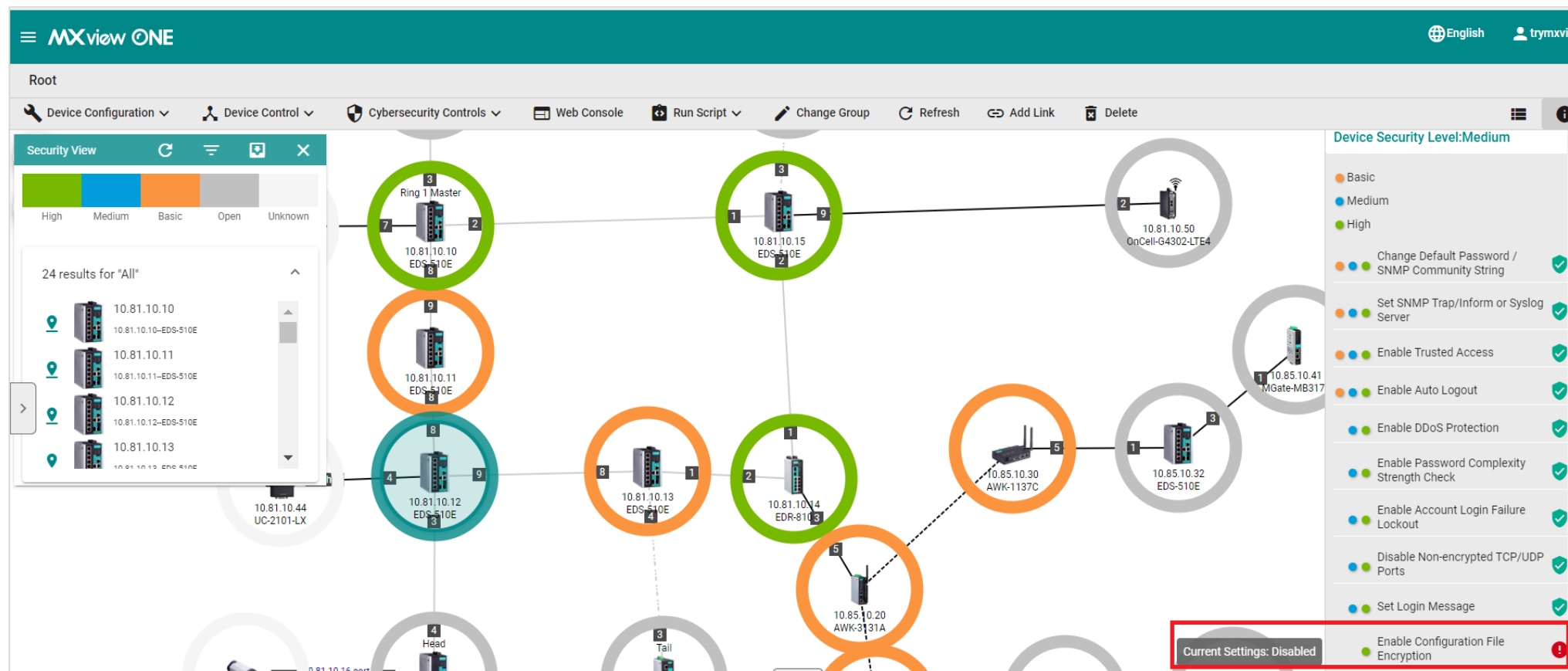
- ☐ Skip
- SNMP Version: v3
- Contact Name: [empty field]
- Location: [empty field]
- Read Community: [empty field]
- Read/Write Community: [empty field]
- Account Name: [empty field]
- Authority: [empty dropdown]
- ☐ Enable account authentication
- Authentication Type: [empty dropdown]
- Authentication Password: [empty field]
- ☐ Enable account privacy
- Privacy Type: [empty dropdown]
- Privacy Password: [empty field]
- v3 Min. Password Length: [empty field]

- ❑ Oprogramowanie do monitoringu, diagnostyki i zarządzania przemysłową siecią Ethernet
- ❑ Zbieranie logów (serwer Syslog), trapów SNMP
- ❑ Alarmowanie (trapy SNMP, e-mail, Teams)
- ❑ Współpraca z urządzeniami innych producentów (SNMP, konieczny plik MIB)
- ❑ Zarządzanie urządzeniami (Import/Export konfiguracji, upgrade firmware, gwarancja)



Security View (zgodność z IEC 62443-4-2)

- ❑ Sprawdza status zabezpieczeń poszczególnych urządzeń
- ❑ Dla wybranego urządzenia podaje informacje, które wytyczne IEC 62443-4-2 są spełnione, a które nie.



The screenshot displays the MXview ONE Security View interface. The top navigation bar includes 'Root', 'Device Configuration', 'Device Control', 'Cybersecurity Controls', 'Web Console', 'Run Script', 'Change Group', 'Refresh', 'Add Link', and 'Delete'. The main area shows a network diagram with devices represented by icons and colored circles indicating their security level: High (green), Medium (blue), Basic (orange), Open (yellow), and Unknown (grey). A list of 24 results for 'All' is shown on the left, including IP addresses and device names like 'Ring 1 Master', 'EDS-510E', 'OnCell-G4302-LTE4', 'MGate-MB317', 'AWK-1137C', 'EDR-8103', 'AWK-3131A', and 'UC-2101-LX'. On the right, the 'Device Security Level: Medium' section lists various security settings with status indicators (green for enabled, red for disabled). A red box highlights the 'Current Settings: Disabled' status for 'Enable Configuration File Encryption'.

Security Level	Device	IP Address
High	Ring 1 Master	10.81.10.10
High	EDS-510E	10.81.10.15
High	EDR-8103	10.81.10.14
Medium	EDS-510E	10.81.10.12
Basic	EDS-510E	10.81.10.13
Basic	EDS-510E	10.81.10.11
Basic	AWK-1137C	10.85.10.30
Basic	AWK-3131A	10.85.10.20
Basic	MGate-MB317	10.85.10.41
Basic	EDS-510E	10.85.10.32
Open	OnCell-G4302-LTE4	10.81.10.50
Unknown	UC-2101-LX	10.81.10.44



- ❑ Topology View, Event View



System

Network and Device

☐	ID	Source	Source IP	Device Alias	Description	Time Issued
	152	MXview One	192.168.127.11	192.168.127.11-EDS-4008-2MSC	Port 4 link up	2025-02-07 12:33:19
	151	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device SNMP reachable	2025-02-07 12:32:55
	150	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device ICMP reachable	2025-02-07 12:32:21
	149	MXview One	192.168.127.11	192.168.127.11-EDS-4008-2MSC	Port 4 link down	2025-02-07 12:32:19
	148	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device SNMP unreachable	2025-02-07 12:32:04
	147	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device ICMP unreachable	2025-02-07 12:31:13
	142	MXview One	192.168.127.11	192.168.127.11-EDS-4008-2MSC	Device SNMP reachable	2025-02-07 11:57:31
	141	MXview One	192.168.127.11	192.168.127.11-EDS-4008-2MSC	Device ICMP reachable	2025-02-07 11:57:30
	140	MXview One	192.168.127.10	192.168.127.10-EDS-4008-2MSC	Device SNMP reachable	2025-02-07 11:57:16
	139	MXview One	192.168.127.10	192.168.127.10-EDS-4008-2MSC	Device ICMP reachable	2025-02-07 11:57:03
	138	MXview One	192.168.127.254	192.168.127.254-NPort-6250-G2	Device ICMP reachable	2025-02-07 11:56:57
	137	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device ICMP reachable	2025-02-07 11:56:55

Serial Port Monitoring

- ❑ Monitorowanie aktywności interfejsu szeregowego

The screenshot displays the ELMARK web interface for configuring serial port monitoring. The main window shows a network diagram with a device labeled '1 (ETH1)' circled in green. A modal dialog titled 'Serial Port Events' is open, showing 'Event Trigger Rules (1/64)'. The rule is configured for 'Serial Port *' with a value of '1'. A dropdown menu is open, listing the following event types: TX & RX Inactivity, TX Inactivity, RX Inactivity, Overrun Error Count, and Parity Error Count. The 'Trigger Threshold *' is set to '1' with a range of '1 - 10000' and a unit of 'Count(s)'. The 'Severity *' is set to 'Warning'. The dialog includes 'Cancel' and 'Apply' buttons at the bottom right.

Root

Device Configuration Device Control Web Console Run Script Change Group Refresh Add Link Delete

Serial Port Events

Event Trigger Rules (1/64)

+ Serial Port * 1

TX & RX Inactivity

TX Inactivity

RX Inactivity

Overrun Error Count

Parity Error Count

Trigger Threshold * 1 1 - 10000 Count(s)

Severity * Warning

Cancel Apply

The diagram illustrates a network topology for a ring configuration. It features two switches, 'Ring 1 Master' and 'Ring 1 Slave', connected in a ring. The 'Ring 1 Master' switch is connected to a laptop (192.168.127.22) via interface 1 and to a server (192.168.127.254) via interface 4. The 'Ring 1 Slave' switch is connected to a laptop (192.168.127.23) via interface 1 and to a server (192.168.127.253) via interface 4. The switches are also connected to each other via interfaces 7 and 8. The IP addresses of the devices are: 192.168.127.22 (laptop), 192.168.127.23 (laptop), 192.168.127.254 (server), and 192.168.127.253 (server). A yellow warning triangle is present in the top right corner.

System	Network and Device
--------	--------------------

☐	ID	Source	Source IP	Device Alias	Description	Time Issued
☐	153	MXview One	192.168.127.254	192.168.127.254-NPort-6250-G2	The RX of serial port 1 did not receive any data in last 1 minute(s).	2025-02-07 12:44:00
☐	152	MXview One	192.168.127.11	192.168.127.11-EDS-4008-2MSC	Port 4 link up	2025-02-07 12:33:19
☐	151	MXview One	192.168.127.253	192.168.127.253-NPort-6450	Device SNMP reachable	2025-02-07 12:32:55
☐		MXview				

Firmware management



➤ Możliwość sprawdzenia Release Notes

➤ Wyświetlanie wersji oprogramowania sprzętowego i statusu modeli w terenie

Wskazówka dotycząca poprawki zabezpieczeń

Select Firmware

Version

6.3

Release Notes

Version

6.3

Change

1. Updated the PT-G7X28 panel image to match the EC version appearance which has no Micro USB on the front panel.

Enhancement

1. [PTP] The PTP domain number will change depending on the parameters of the PTP profile.

Feature

N/A

Fix

1. [PTP] The "UTC Offset Valid" field shows incorrectly on the System Time page.

2. [PTP] The path delay is calculated twice.

3. [PTP] The system does not send inaccurate power profile TLV received from the Master to the Slave.

4. [PTP] When the device is configured for one-step sync but receives two-step sync, the correction field is not properly updated.

5. [OpenSSL] [CVE-2022-0778] Vulnerability in OpenSSL.

6. [PoE] Navigating to the PoE Diagnostic page through HTTPS causes a memory leak.

7. [Fiber Check] TX/RX power warnings are shown on the SFP-RJ45 module.

8. [Fiber Check] The event for low RX power does not trigger correctly.

9. [MMS] The character restrictions for the IED name are not applied.

10. [MMS] Changing the IED name will cause the system to reboot.

11. [PoESE Check] The PoESE triggered port event is recorded incorrectly in the event log.

Cancel

Select

MXview ONE

Type keyword to search

Dashboard

Topology

Device Discovery

Device Management

Saved CLI Scripts

Firmware Management

Device Configuration Center

Event Management

Notification Management

Reports

Integration

Administration

Help

Firmware Management

Check Firmware Status

Moxa Firmware Server Status: Connected

Last Checked: 2024/01/16 PM 11:48:18

Check Interval: N/A

Check Now

Enable Check Interval

Models

Ignored Models

	Model Series	Device Status	Latest Version on the Firmware Server	Selected Version	Selected Firmware Download Status
☐	EDS-408A	Not updated	v3.13	None	
☐	EDS-G512E-8PoE	Not updated	v6.4	None	
☐	PT-G510	Not updated	v6.5	None	
☐	PT-G7728	Partially updated	v6.3	v6.3	
☐	AWK-1151C	All updated	v2.0	None	
☐	AWK-3252A	All updated	v2.0	None	
☐	AWK-4252A	All updated	v2.0	None	
☐	EDS-4012-8P-4GS	All updated	v3.2	None	
☐	EDS-G4008	All updated	v3.2	None	

Firmware management



➤ Wybierz urządzenia

Select Devices

IP	Alias	Model Series	Current Version	Selected Version
☐ 1.1.1.5	1.1.1.5-PT-G7728	PT-G7728		v6.3
☒ 192.168.127.29	192.168.127.29-PT-G7728	PT-G7728	V6.2 build 21110316	v6.3
☒ 192.168.127.25	192.168.127.25-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
☐ 1.1.1.6	1.1.1.6-PT-G7728	PT-G7728		v6.3
☒ 1.1.1.7	1.1.1.7-PT-G7728	PT-G7728		v6.3
☐ 192.168.127.26	192.168.127.26-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
☐ 192.168.127.27	192.168.127.27-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
☒ 192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E	V6.4 build 23102508	v6.4

Cancel Next

Upgrade Sequence

Update Mode
Strict Sequential

Order	IP	Alias	Model Series	Current Version	Selected Version
1	192.168.127.11	192.168.127.11-EDS-G516E	EDS-G516E	V6.4 build 23102508	v6.4
2	192.168.127.25	192.168.127.25-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
3	192.168.127.26	192.168.127.26-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
4	192.168.127.27	192.168.127.27-PT-G7728	PT-G7728	V6.3 build 22120913	v6.3
5	192.168.127.29	192.168.127.29-PT-G7728	PT-G7728	V6.2 build 21110316	v6.3

Cancel Scheduled Upgrade Upgrade Now

➤ Aktualizacja wg harmonogramu lub na żądanie



Recently Released	
TITLE	LAST UPDATED ▾
NPort W2150A/NPort W2250A Serial Device Servers Vulnerabilities	Dec 13, 2018
Moxa's Response Regarding the Libssh Authentication Bypass Vulnerability	Nov 27, 2018
ThingsPro 2 Series System Software Vulnerabilities	Oct 17, 2018
EDR-810 Series Secure Router Vulnerability	Oct 24, 2018
Moxa's Response Regarding the Intel Management Engine Vulnerability	Oct 24, 2018
NPort 5200 Series Serial Device Servers Vulnerabilities	Oct 24, 2018
EDS-G508E Series, EDS-G512E Series, and EDS-G512E Series Vulnerabilities	Oct 24, 2018

SUMMARY										
MiiNePort E1/E2/E3 Series Serial Device Server Vulnerabilities Version: 1.0 Release Date: Jul 01, 2016 Reference: ICSA-CERT, ICSA-16-145-01 Multiple product vulnerabilities were identified in Moca's E1/E2/E3 Series Serial Device Server. In response to this, Moca has developed related solutions to address these vulnerabilities. The identified vulnerability types and potential impacts are shown below: <table> <tr> <th>ITEM</th><th>VULNERABILITY TYPE</th><th>IMPACT</th></tr> <tr> <td>1</td><td>Clear text storage of sensitive information</td><td>Disclosure of sensitive information</td></tr> <tr> <td>2</td><td>Cross-site request forgery</td><td>Unauthorized HTTP requests may allow attacker to trick user into making unintentional request</td></tr> </table>		ITEM	VULNERABILITY TYPE	IMPACT	1	Clear text storage of sensitive information	Disclosure of sensitive information	2	Cross-site request forgery	Unauthorized HTTP requests may allow attacker to trick user into making unintentional request
ITEM	VULNERABILITY TYPE	IMPACT								
1	Clear text storage of sensitive information	Disclosure of sensitive information								
2	Cross-site request forgery	Unauthorized HTTP requests may allow attacker to trick user into making unintentional request								

- Szczegółowość i wpływ podatności
- Lista produktów, których dotyczy problem
- Sugerowane rozwiązanie

Szybkie rekomendacje



Upewnij się, że wszelki
możliwy dostęp jest
zablokowany

Okresowo sprawdzaj, czy nie trzeba
załatać żadnych dziur

Nie zostawiaj otwartych drzwi

Poradniki – konfiguracja funkcji bezpieczeństwa



FAQ



Cybersecurity FAQ for Moxa Edge Devices

1. Introduction

While companies are tapping into the opportunities that the Industrial Internet of Things (IIoT) has to offer, digitalization has become a key initiative for industries. Digitalization has allowed the industrial control system (ICS) landscape to develop quickly in recent years. Originally, ICS networks were physically isolated and almost immune to cyberattacks. However, recently, there has been a rise in the sophistication of cyberattacks, which has prompted everyone from IT to OT personnel to produce solutions that enhance industrial cybersecurity. Thus, understanding industrial cybersecurity requirements will help companies mitigate cybersecurity risks. This FAQ collects the questions Moxa has been asked in past few years and also our responses to help the distributors, system integrators and customers to understand how Moxa products can help him to protect his network from cyberattacks.

2. Frequently Asked Questions

2.1 Well-known Vulnerabilities Sharing



1. In October 2018, Apple, Google, Microsoft and Mozilla announced that they're going to disable the support of TLS v1.0/v1.1, will this affect the web consoles of Moxa devices?



The web consoles of Moxa devices will start to support TLS v1.2 by default after new firmware release end of 2020. The new firmware will also provide the ability to enable TLS v1.0/v1.1 (default disabled) to fulfill the users who are still using the old operation systems which may only support TLS v1.0/v1.1.

Technical Note



The Configuration Management and Hardening Guide of Moxa's NPort 5000 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

Technical Note



The Configuration Management and Hardening Guide of Moxa's NPort 6000 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

Technical Note



The Configuration Management and Hardening Guide of Moxa's MGate MB3170/3270/3660/3280/3480 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

Technical Note



The Configuration Management and Hardening Guide of Moxa's MGate 5000 Series

1. Introduction

We, Moxa, understand that more and more of Moxa's customers are concerns about the security of their network system and even on the individual devices. Moxa is committed to cybersecurity and endeavor to make the products as secure as possible. In order to support Moxa's customer to meet certain security guidelines and frameworks, this document is intended to provide general guidance on how to configure and secure the installation of Moxa devices.

Within this document, the recommended steps for securing a Moxa device are guided. The steps provided are recommendations as the applications are various from Moxa's customer. As it is a general document, these recommendations are some good practices for most of the applications. However, to ensure the recommended settings are applicable to your environment without creating a conflict and affecting your application, it's highly suggested to review and test the configuration thoroughly before implementing on the production system.

FAQ – najczęściej
zadawane pytania

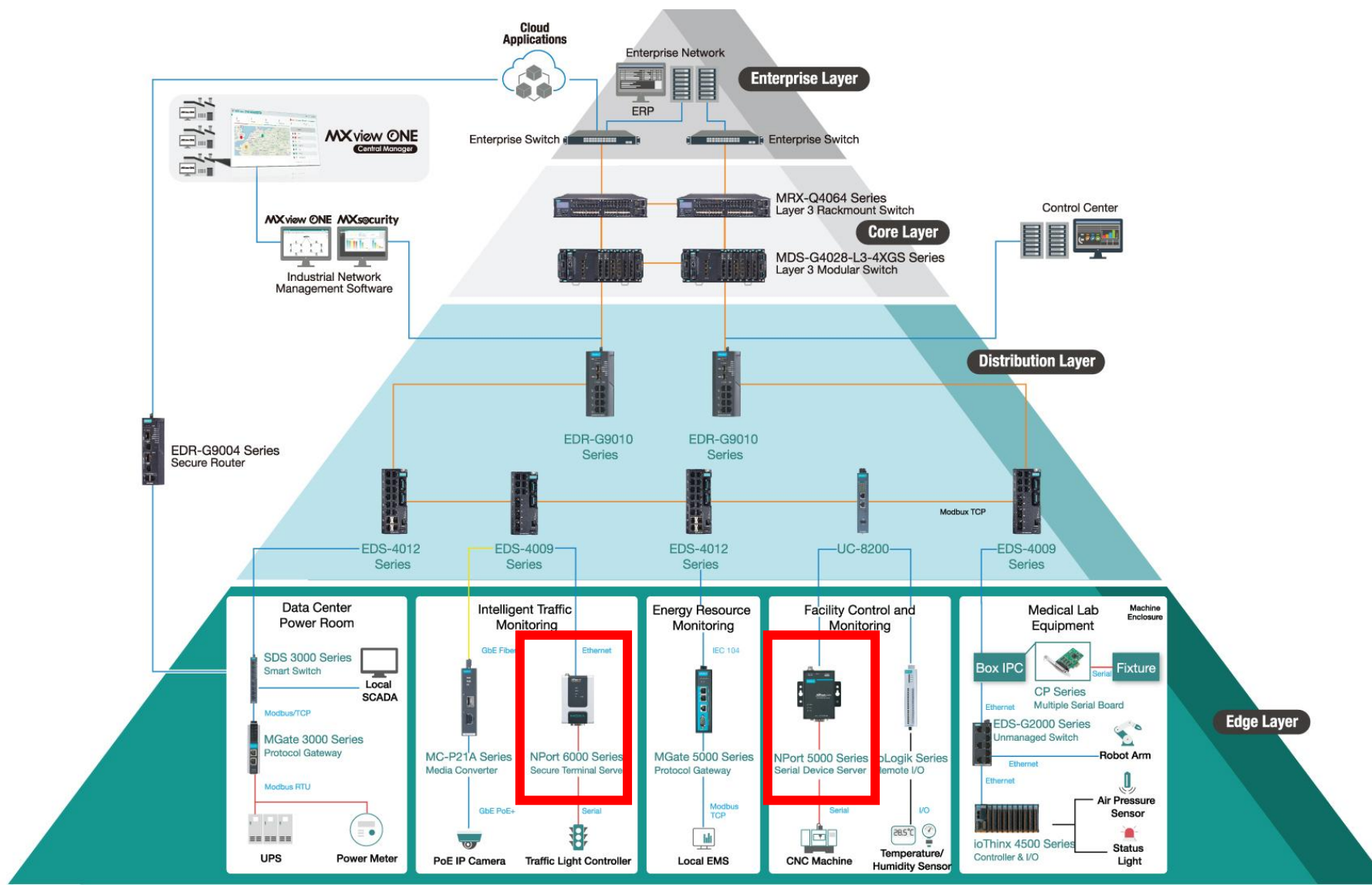
NPort 5000

NPort 6000

MGate MB3000

MGate 5000

Kompleksowe portfolio MOXA





Dziękuję za uwagę

Sprawdź:

www.elmark.com.pl