NOX Security Whitepaper

Version 16.0
07-02-2022

Indhold

NOX BUS

NOX bussen er af type RS-485 Standard.

NOX bussen benytter obfuskering/sløring af data ved kommunikation mellem CPU og NOX enheder, udviklet af NOX Systems.

Alle besked skifter form fra gang til gang de benyttes, og det er derfor meget kompliceret at skulle simulere/emulere en besked, og afspille denne tilbage på NOX bussen.

NOX bussen indgår som en del af NOX systemet, og har ikke nogen indflydelse på IT-infrastrukturen, den udføres som en selvstændig del af selve NOX installationen.

Ved afbrydelse af bussen vil NOX systemet generere en sabotage alarm for alle manglende enheder.

Ved forsøg på manipulation med datapakker vil disse blive ignoreret da de ikke indeholder den korrekte datastruktur.

NOX IP BUS / NOX MXA

NOX IP BUS / NOX MXA består af 2 enheder:

1 stk. Moxa 5110A
1 stk. NOX RPT

Der oprettes en forbindelse direkte fra NOX CPU til Moxa enheden til IP Adressen på Moxa enheden.

Kommunikationen mellem NOX CPU og Moxa enheden er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85. Fra R7 (Version 10.0) benyttes der 256 AES kryptering.

Kommunikationen forgår på følgende porte: 4001

Porten er anbefalet men kan frit ændres.

Moxa enheden forbindes via RS232 til NOX RPT og derved konverteres IP bussen til en RS485 NOX bus, med de samme egenskaber som er beskrevet under NOX BUS afsnittet. Ved netværksfejl mistes kontrollen med enhederne helt, indtil netværksfejlen er udbedret.

NOX Master/Slave

NOX Master/Slave forhold, består af 2 eller flere NOX CPU som kommunikerer via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Kommunikationen foregår på følgende porte: 8981

Porten er låst og kan ikke ændres.

NOX Redundant CPU

NOX Redundant CPU, består af 2 NOX CPU som kommunikerer via TCP/IP, de er 1 til 1 dubleret, samt deler fysiske busser, således at der ved genstart eller nedbrud af den ene, tager den anden over uden afbrydelser. Al kommunikation mellem primær og sekundær CPU foregår uden kryptering.

Kommunikationen foregår på følgende porte: 8982

NOX PC Control

NOX PC Control er betjeningssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX PC TPA

NOX PC TPA er betjeningssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX Logger

NOX Logger er et lille stykke software som kan køre uafhængigt af NOX Config eller NOX PC Control, egenskaberne for dette program er at opsamle logs i real-time gennem NoxDLL.dll.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85 (**NOX Logger 3.0**)

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering. (**NOX Logger 4.0**)

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1) samt skal følgende filer inkluderes i mappen med NOX Logger:

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

NOX Config

NOX Config er konfigurationssoftware som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4321, 4322, 6251

Portene er låst og kan ikke ændres.

NOX SIMS V6

SIMS er en Server/Client software løsning for multicentral- og grafisk løsning med mulighed for integration gennem SQL Server. SIMS betyder Security Information Management System.

Server:

Kommunikationen mellem SIMS Server og NOX CPU'er, er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering og TLS 1.2 (SSL)

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1) og .NET 4.5

Kommunikationen foregår på følgende porte: 4322

Porten er låst og kan ikke ændres.

Client:

Kommunikationen mellem SIMS Client og SIMS Server er beskyttet med en 128 bit AES kryptering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1) og .NET 4.5

Kommunikationen foregår kun mod SIMS Serveren på følgende porte: 2010

Port 2010 er anbefalet men kan frit ændres.

iNOX & NOX for Android

iNOX og NOX for Android er Smartphone apps som kan tilgå NOX CPU via TCP/IP.

Kommunikationen er beskyttet med en 384 bit Blowfish kryptering, i alle Firmware versioner til og med Version 9.85

Fra R7 (Version 10.0) benyttes 256 AES kryptering.

Fra version 10.0 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Softwaren kan installeres på alle Windows versioner, 32 bit og 64 bit, fra Windows 7 og frem.

Forudsætningen for fuld funktionel software er præ-installation af .NET 2.0 (inkluderet i .NET 3.5.1)

Kommunikationen foregår på følgende porte: 4325

Porten er anbefalet men kan frit ændres.

NOX SSH

NOX SSH er kun SSH Server, kommunikationen kan vælges at være mellem 256 bit til 4096 bit Diffie Hellman, Private Key auth eller Public Key auth.

For yderligere information henvises til Rebex hjemmeside, www.rebex.net, Rebex File Server -> Features -> SSH Server

NOX PCIF (Generel beskyttelse af PC Interface)

Brute force forhindring (Forhindre gentagne forsøg med forkert kode over IP)

I R6 (<9.85x):

IP Interfacet følger de angivne antal forsøg og tid, som er valgt i NOX Config under "Generelt -> Indstillinger -> Bruger -> Betjeningsspærring" ved opnået antal forsøg, spærres IP Interfacet for den pågældende Source IP i det antal minutter der er angivet (standardtid = 3 minutter).

I R7 (>10.0):

SL3: (Bagud kompatibel tilstand med kode alene)

IP Interfacet følger de angivne antal forsøg og tid, som er valgt i NOX Config under "Generelt -> Indstillinger -> Bruger -> Betjeningsspærring" ved opnået antal forsøg, spærres IP Interfacet for den pågældende Source IP i det antal minutter der er angivet (standardtid = 3 minutter).

SL4: (Høj sikkerhed, autentifikation gennem brugernavn og adgangskode, TLS 1.2)

1. Det anbefales at benytte adgangskoder med høj kompleksitet. Kravet til kompleksitet sættes op i NOX Config under "Generelt -> Indstillinger -> Netværksadgang/Netværksnøgle -> Password regler"

2. For hvert forkert loginforsøg sættes der en forsinkelse på 1 ms, dette øges op til 1 sekund, således det vil tage uforholdsmæssigt lang tid at "gætte" koden. Denne forsinkelse fjernes først ved korrekt login.

Kombinationen mellem komplekse koder og forsinkelse betragtes som en særdeles sikker beskyttelse mod Brute force forsøg.

NOX Kode politik (betjeningsenheder på NOX BUS)

Standard konfigurationen spærrer alle betjeningspaneler i 3 minutter ved 5 forkerte kode indtastninger, efterfølgende spærrer alle paneler i 5 minutter ved indtastning af 6. forkerte indtastning. Det er beskrevet i Forsikring og Pensions (F&P) retningslinjer for AIA anlæg, at det skal være sådan.

I NOX er det programmerbart, så hvis man ønsker en strammere kode politik er det muligt.
Vi fraråder at man lemper politikken, da det medfører at anlægget ikke længere lever op til F&P's krav.

NOX Kort + PIN kode politik (CMx interfaces på NOX BUS)

Ved forkert PIN Kode indtastning, er standard opsætningen at der ikke sker noget.
Det er en programmerbar funktion, og den er ikke omfattet af regler som ovenstående fra F&P.

I praksis betyder det at hvis man ønsker at et kort spærres efter 3 forkerte PIN indtastninger, er det muligt.

Et spærret kort kan efterfølgende åbnes af en person som kan redigere brugere gennem PC Control.

Dataflow/Båndbredde forbrug

SIMS Server -> SIMS Client

Kommunikationen mellem SIMS Server og SIMS Client består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Der er et større behov når man tilslutter en SIMS klient til SIMS Server første gang, da der overføres plantegninger. Disse tegninger caches på klienten, og synkroniseres ved ny forbindelse, såfremt der er sket ændringer.

Hver gang der er en hændelse i NOX Systemet sendes denne til SIMS Serveren, herfra sendes den videre til aktive klienter. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem SIMS Server og SIMS Client er 2 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 256 hændelser i sekundet. Ved større SIMS installationer med >50 NOX CPU'er kan det være nødvendigt med en højere båndbredde.

NOX CPU -> SIMS Server

Kommunikationen mellem NOX CPU og SIMS Server består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Hver gang der er en hændelse i NOX Systemet sendes denne til SIMS Serveren. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem NOX CPU og SIMS Server er 0,5 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 64 hændelser i sekundet.

NOX CPU -> NOX Config/NOX PC Control

Kommunikationen mellem NOX CPU og NOX Config/NOX PC Control består af krypteret data, mest af alt hændelser (tekst), det kræver nærmest ingen båndbredde.

Hver gang der er en hændelse i NOX Systemet sendes denne til aktive klienter. Hver hændelse består af max. 1 kB data, en hændelse er en kobling, alarm, bevægelse, osv.

Den anbefalede båndbredde mellem NOX CPU og SIMS Server er 0,5 Mbit/s, som vil dække langt de fleste tilfælde, da det svarer til 64 hændelser i sekundet.

Ekstern Applikation -> NOX

Der findes mange typer indgående forbindelsesmuligheder til NOX, fælles for dem er at de typisk er tekstbaserede, derfor kræver de nærmest ingen båndbredde. Nogle af disse muligheder tilbyder også kryptering (SSH/SDK). Da det er variabelt hvad man ønsker at sende til NOX vil det være nødvendigt at lave en vurdering fra sag til sag. Vores erfaring er dog at 2 Mbit/s vil være nok i 99 ud af 100 tilfælde.

GDPR Compliance på NOX

GDPR bør håndteres med omtanke i forbindelse med AIA og ADK, da de tjener forskellige formål hver især.

AIA og ADK er skabt til at logge al aktivitet for at sikre mod Tyveri, adgang for uvedkommende i udvalgte områder, Terror sikring og den slags. NOX er et godkendt integreret AIA og ADK anlæg, i henhold til EN50131 standarden.

GDPR er skabt til at beskytte private data, og sikre at disse er ejet af personen selv. Således kan en person bede om at blive glemt i forhold til bestemmelserne i GDPR artikel 17.

Under normale omstændigheder vil et AIA/ADK anlæg ikke tilbyde mulighed for at udnytte denne bestemmelse, da de er designet til netop ikke at kunne manipuleres.

I NOX er det dog muligt at anonymisere brugere i PC Control, fra NOX Config version R8 for operatører med ret til at slette brugere.

VI anbefaler at der benyttes et minimum af personfølsomme eller personhenførbare data i systemet. Vores anbefaling er maksimalt at benytte, Fornavn, Efternavn og initialer.

Vær opmærksom på at dette medfører et brud på bestemmelserne for EN50131 at manipulere loggen, og derfor kan påvirke et eventuelt krav til virksomhedens sikringsniveau og forsikringskrav. Nedenstående uddrag af EN50131 bestemmelsen omhandlende håndtering af hændelses logning:

Table 21 – Event recording – Memory

Capacity & endurance	Grade 1	Grade 2	Grade 3	Grade 4
Memory capacity – Minimum number of events	Op	250 events	500 events	1 000 events
Minimum endurance of memory after I&HAS power failure	Op	30 days	30 days	30 days
Key: Op = Optional.				

I NOX systemet er minimumsindstillingerne:

- 2000 Alarm loghændelser
- 2000 Intern loghændelser
- 6000 Bruger loghændelser

Det er ikke teknisk muligt at reducere dette antal.

Anbefalinger

For at imødekomme kravene vedr. GDPR har vi følgende informationer og anbefalinger til brug for implementering af GDPR Compliance i sammenhæng med NOX:

1. NOX gemmer fra 6000 brugerhændelser op til 100.000 på centralen. Når maksimal grænsen er nået, vil det være "First in, First out" der gælder. Da det er et antal loghændelser der skal opnås for at overskrive en enkelt hændelse vil det ikke være muligt at give et entydigt svar på hvor længe systemet gennem logs. Det vil bero på firmaets størrelse, og hvor mange gange hver medarbejder går gennem dørene pr. dag. Vi kan oplyse at hver gang der gives en godkendt adgang skrives der 3 hændelser i loggen.

2. Persondata der indgår i brugerlogs er afhængig af hvordan man stykker sine brugernavne sammen i NOX. Normalt vil det være <Fornavn Efternavn> og et kortnummer der indgår, altså ingen telefonnumre, personnumre eller andre følsomme data. Et eksempel kan også være at der benyttes AD som integration. I så fald vil et brugernavn blive stykket sammen af ”Fornavn Efternavn (Initialer)” se eksempel på hvordan en logentry ser ud her:

30.01.18 11:52:16 logind ved CMU af John Doe (JDO)
30.01.18 11:52:16 område Door Entrance ændret til Adgang Godkendt (5) af John Doe (JDO)
30.01.18 11:52:21 område Door Entrance ændret til lukket af automatic

3. Al data og logs på NOX Systemet er krypteret med en AES-256 algoritme, det er kun muligt at tilgå logs gennem NOX egne applikationer, eller gennem SSH2.

Alle operatørlogins gemmes i brugerloggen på lige fod med adgang til områder og døre.

Operatør logning indeholder, Hvem loggede ind, og ændringer af tilstande i systemet (til-/frakoblinger, o. lign.) samt evt. ændringer af brugere.

GDPR Compliance på SIMS

Hvis man benytter SIMS Software, vil ovenstående punkt, **GDPR Compliance på NOX** være gældende med følgende tilføjelser.

SIMS gemmer alle loghændelser i en SQL-database, her vil antallet være væsentligt højere end den begrænsning der findes i NOX systemet. I SIMS er det til gengæld muligt at definere en maksimal opbevaringstid for loghændelser pr. alarmtype, standardtiden for opbevaring er 365 dage, men er frit valgbar.

Da SIMS gemmer alle informationer i en SQL-Database, vil det være muligt at anonymisere enkelt loghændelser med en forholdsvis enkel SQL Query, og således kunne opfylde et evt. ønske om at blive ”glemt”.

Det er muligt at få udleveret et eksempel på en Anonymiserings SQL Query, samt få hjælp til at udføre en evt. anonymisering ved henvendelse til installatøren af NOX/SIMS systemet eller ARAS Security A/S.