

## NOX Security Whitepaper

Version 10.0  
23-05-2018

### Indhold

NOX BUS.....	2
NOX IP BUS / NOX MXA .....	3
NOX PC Control.....	4
NOX Logger.....	4
NOX Config .....	5
NOX SIMS V6 .....	6
iNOX & NOX for Android .....	7
NOX SSH .....	8
NOX PCIF (Generel beskyttelse af PC Interface).....	9
Dataflow/Båndbredde forbrug.....	10
GDPR Compliance på NOX .....	11
GDPR Compliance på SIMS.....	12
Generelt om GDPR ved brug af NOX/SIMS .....	13

## NOX BUS

NOX bussen er af type RS-485 Standard.

NOX bussen benytter obfuscering 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 og med Firmware version 9.89 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 afbrydelse af IP bussen vil NOX systemet generere en sabotage alarm for alle manglende enheder.

## 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

Alle fremtidige versioner fra version 9.89 vil benytte 256 AES kryptering.

Fra version 9.90 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software 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

Der findes ikke en udgave af Noxlogger efter NOX version 9.85.

Software 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:

Compression.dll  
Bitmanipulation.dll  
Noxdll.dll  
NoxLoggerV30.exe

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

Alle fremtidige versioner fra version 9.89 vil benytte 256 AES kryptering.

Fra version 9.90 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software 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

Alle fremtidige versioner fra version 9.89 vil benytte 256 AES kryptering og TLS 1.2 (SSL)

Fra version 9.90 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software 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.

Software 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, 443

Port 2010 er anbefalet men kan frit ændres. Port 443 er låst og kan ikke 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

Alle fremtidige versioner fra version 9.89 vil benytte 256 AES kryptering.

Fra version 9.90 er det muligt at tilvælge højere sikkerhed gennem certifikat baseret autentificering, eller brugernavn og adgangskode autentificering.

Software 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](http://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 (>9.94m):

#### 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: (Ny og ekstra sikker 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.

## 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 er en anderledes størrelse i NOX (AIA/ADK) sammenhænge, da de to er modstridende i deres ophav.

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.

Altså vil et AIA/ADK anlæg pr. teknisk definition ikke give mulighed for at udnytte "retten til at blive glemt" iht. GDPR.

Det er pr. design ikke muligt at slette en eller flere enkeltstående hændelse(r) i systemet.

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

Hvis der bliver stillet et krav at skulle slette logs i systemet, vil det være muligt for installatøren at få adgang til at slette ALLE loghændelser i systemet på opfordring.

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

**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 teknisk ikke 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 enkelt 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.

## Generelt om GDPR ved brug af NOX/SIMS

Anbefalingen for at leve op til GDPR vil være at man oplyser de dele af ovenstående som er relevante for jer i et tillæg til ansættelseskontrakten, og henviser til at det er hensynet til beskyttelse af virksomhedens aktiver, beskyttelse mod sabotage, industrispionage og beskyttelse af virksomhedens personale der danner grundlag og vægtes for denne datahåndterings metode. Graden af alvorlighed og vægtning af loghistorik, må bero på en sikkerhedsvurdering fra virksomheden selv.

GDPR er en levende proces, og vi ser på forskellige muligheder for at hjælpe installatørerne og kunderne til at opnå en enklere håndtering af deres AIA/ADK når det kommer til persondataforordningen, det skal dog altid sammenholdes med at NOX er et Sikkerhedssystem i højeste godkendelsesklasse, og det vil altid være sikkerheden i systemet der kommer i første række.

På længere sigt er det hensigten at tilbyde mulighed for direkte anonymiseringer i både NOX og SIMS.

I begge tilfælde vil det blive udført som valgfrie optioner, og vil blive inkluderet i en fremtidig opdatering.

I tilfældet NOX skal det understreges en sådan funktion ikke er i overensstemmelse med EN50131, og derfor heller ikke er i overensstemmelse med de eventuelle krav der er stillet fra Forsikring og Pension (F & P) til virksomheden.