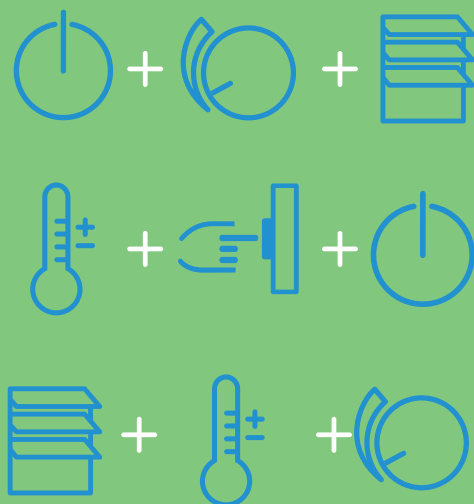


KNX MIX2-actoren
Upgrade naar KNX Data Secure
Whitepaper



Safety first!

KNX-installaties met KNX Data Secure veilig plaatsen en gebruiken



Open standaarden zoals KNX zijn een absolute vereiste voor een betrouwbare investering in de automatisering van een gebouw. Nog meer flexibiliteit bieden modulaire systemen, die voordelig kunnen worden uitgebreid. De beste oplossingen maken zelfs het gebruik van nieuwe standaarden zoals KNX Data Secure mogelijk, zonder dat alle actoren moeten worden vervangen.



Imagoverlies is vergeleken met gevaren voor lijf en leven nog een geringer probleem, wanneer het gebouwbeheersysteem in openbare gebouwen zoals in een beursshal wordt gehackt en systemen worden lamgelegd.

Door automatisering en netwerkkoppeling zijn besturingen en elektrische installaties veel krachtiger, efficiënter en comfortabeler geworden. Tegelijkertijd is de afhankelijkheid van een steeds complexere techniek toegenomen. Elke installateur kan een beveiligingsschakeling begrijpen en onderhouden. Bij een uitval gaat het meestal om slechts een klein gedeelte van de installatie. Een omvangrijke automatiseringsoplossing kan bij een storing echter de hele installatie lamleggen. Bovendien is de gebruiker aangewezen op speciale bedrijven en hooggekwalificeerde deskundigen. Vooral in eigen beheer ontwikkelde systemen blijken dan vaak enorm kostbaar te zijn. Dit heeft geleid tot de opmars van open systemen, waarmee producten van verschillende fabrikanten kunnen worden gebruikt. Bovendien wordt de voorkeur gegeven aan modulaire systemen, zoals Remote-IO-modules in de industrie, boven vaste apparatuur. Dat geldt ook voor de gebouwautomatisering. Hier ziet men vergelijkbare ontwikkelingen zoals in de industrie. Dat geldt helaas ook voor een onplezierig bijverschijnsel van de automatisering: de kwetsbaarheid ten opzichte van hackers.

De vijand in huis

In moderne, via netwerken gekoppelde besturingen zijn hiaten voor criminelen ontstaan, die enkele jaren geleden nog totaal ondenkbaar waren. Een van deze methoden is de diefstal van gegevens, wanneer iemand zich als koper voordoe. Nog eenvoudiger is de versleuteling van databases of gewoon sabotage. Hackers leggen computercentra of fabrieken lam, waarbij aanzienlijke bedragen worden afgeperst. De verantwoordelijken leveren intussen enorme inspanningen om hun installaties tegen aanvallen van buitenaf te beschermen. Zo heeft het beheersysteem van een productieafdeling vaak zijn eigen netwerken, die alleen op enkele, scherp bewaakte interfaces met de bedrijfs-IT verbonden zijn. Maar welk nut heeft een beveiligde machinebesturing als de verlichting of de airconditioning in een productievestiging uitvalt? Vanwege de schade die hackers aanrichten, ontstaat ook bij de gebouwautomatisering een onbehaaglijk



Gevaren voor openbare of commerciële gebouwen liggen voor de hand: wanneer bijvoorbeeld tijdens een beurs of concert de halventilatie uitvalt, of in de productievestiging de verlichting niet meer werkt, dreigt onmiddellijk een grote economische schade. Ook kan de reputatie duurzaam worden aangetast.

De achterdeur van het netwerk

„Idealiter heeft men toegang tot de groene kabel nodig, maar zelfs een slecht afgeschermd gasten-wifi kan gevaarlijk zijn”, beschrijft Michael Saile van Productmanagement Building Automation bij Theben AG een mogelijk aanvalsscenario. De uitgangssituatie in een gebouw verschilt aanzienlijk van een aanval op de bedrijfs-IT. Daarbij handelen de daders meestal vanuit het buitenland. In principe is dit ook bij een gebouw mogelijk, wanneer het KNX-netwerk is uitgerust met een IP-interface of een IP-router. Ook een visualisatie, die zowel met het internet als met de KNX-BUS verbonden is, biedt aanvalsmogelijkheden. Vele ontwerpers zien daarom af van één, ten minste altijd actieve interface met het internet. Een aanval van buiten het perceel is dan onmogelijk. Ook een dergelijke configuratie is echter niet 100% veilig: in relatief vrij toegankelijke gebouwen, zoals beurshallen of hotels, kan de bezoekersstroom gewoon niet volledig worden gecontroleerd. Een aanvaller kan gemakkelijk het gebouw binnenkomen en profiteert dan van het feit dat de busnetwerken nauwelijks tegen manipulaties zijn beschermd, in tegenstelling tot de IT. Omdat er in bijna elk kantoor fysiek openbaar toegankelijke Ethernet-aansluitingen zijn, wordt het netwerk met wachtwoorden en overige maatregelen beveiligd. Maar wie denkt al aan de schijnbaar ontoegankelijke bussen van de gebouwautomatisering? Daarvoor is het al voldoende om in een berg-ruimte of een wc de afdekplaat van het verlaagde plafond op te tillen. Verkleed als onderhoudsmonteur of schoonmaker is dit zelfs op openbare plaatsen mogelijk. Na enkele pogingen weet men de beveiliging wel te vinden. De opvallende groene kabels zijn zelfs voor leken gemakkelijk te herkennen. Zo kan met slechts enkele handelingen een mobiele telefoonmodule worden geïnstalleerd, waarmee de aanvaller permanent toegang heeft tot de datastroom. Het gevaar om ontdekt te worden, is klein. En zelfs wanneer de modem per ongeluk wordt gevonden, is het bijna onmogelijk de dader op te sporen.

Bij een modem zijn er zelfs meerdere aanvalsmogelijkheden. De grove methode is de bus te 'jammen', d.w.z. overbelasten met gegevens tot aan 'Denial of Service'. Dit leidt tot een totale uitval van de gebouwautomatisering. Iets subtieler is de andere methode: met de modem kan het dataverkeer gedurende een langere periode worden geregistreerd. Een deskundige kan daaruit conclusies over de functies trekken en vervolgens gericht de besturing overnemen, bijv. de ventilatie uitschakelen. Dit is met name fataal wan-



Zelfs een slecht afgeschermd gasten-wifi kan gevaarlijk zijn.

- Michael Saile
Productmanagement
Building Automation
Theben AG

neer veiligheidsrelevante functies via KNX worden aangestuurd, bijvoorbeeld deuropeners, alarminstallaties of het toegangsbeheer. Gelukkig heeft de KNX Association ook al op dergelijke scenario's gereageerd.

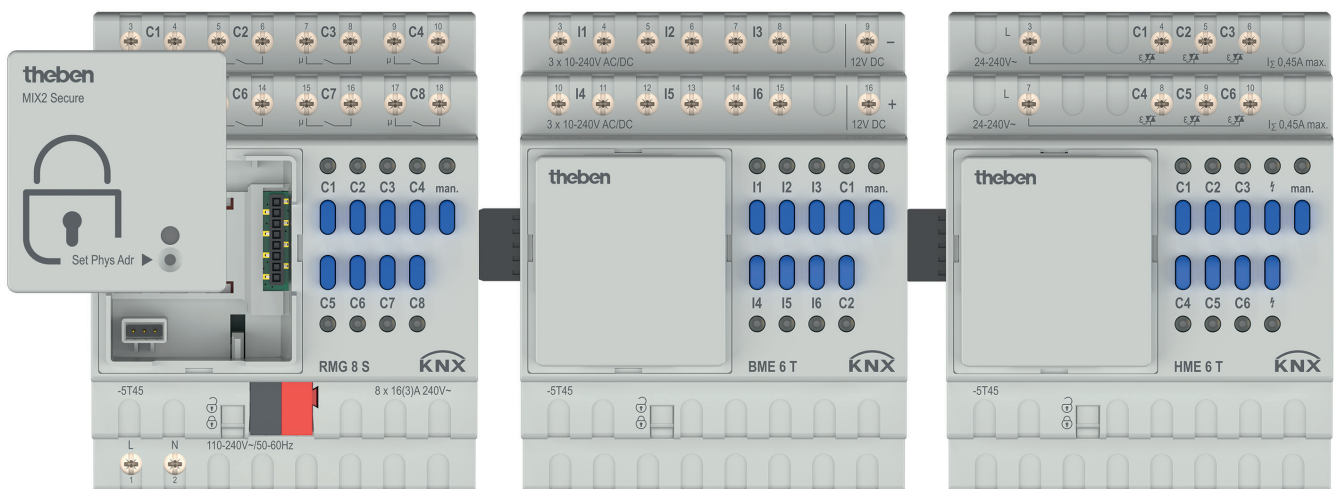
Veiligheid voor KNX

Vanwege de mogelijke bedreigingen heeft de KNX Association de standaard KNX Secure ontwikkeld. Deze technologie is conform EN 50090-3-4 gestandaardiseerd en voldoet aan de strengste versleutelingseisen conform ISO 18033-3, zoals de AES 128 CCM-versleuteling. Digitale aanvallen worden zo aanzienlijk moeilijker, zo niet onmogelijk. KNX Secure bestaat uit twee modules, KNX IP Secure en KNX Data Secure. KNX IP Secure breidt het IP-protocol zodanig uit dat alle overgedragen telegrammen en gegevens volledig versleuteld zijn. KNX Data Secure beschermt gebruikersgegevens door versleuteling en authenticatie tegen toegang en manipulatie door onbevoegden.

Het nadeel van KNX Secure zijn de eisen aan de hardware. Michael Saile legt uit: „Je kunt een bestaand apparaat niet gewoon ombouwen. Daarvoor heb je grotere processoren, meer geheugen etc. nodig, dus een nieuwe generatie apparaten. Bij nieuwe apparaten zullen de aanbieders daarmee rekening houden, maar dat kan nog wel even duren. Wij zijn bij Theben met in totaal 23 producten al ver gevorderd.“ Bijzonder interessant zijn de MIX2-actoren, waarmee gebruikers KNX Data Secure gemakkelijker naderhand kunnen installeren.

KNX Data Secure gewoon naderhand installeren

MIX2-actoren van Theben bieden een zeer hoge flexibiliteit bij het ontwerp en bij wijziging van het gebruik. Het systeem bestaat uit diverse basisapparaten met een buskoppeling, waarop maximaal twee uitbreidingsmodules kunnen worden aangesloten. Zo kan het aantal uitgangskanalen per busmodule worden verdrievoudigd, en dat met de meest uiteenlopende functies zoals het schakelen en dimmen van de verlichting, aansturen van de zonwering of regelen van de verwarming. Dat bespaart ruimte en kosten. De buskoppeling in het basisapparaat kan indien nodig snel en eenvoudig worden vervangen. Dat is ook



Uitneembare intelligentie: Alleen de KNX MIX2-basismodule beschikt over een buskoppeling, waarop de uitbreidingsmodules kunnen worden aangesloten. Indien nodig, kan deze eenvoudig worden verwijderd en vervangen.



MIX2 is al tien jaar Data Secure ready.

- Axel Kaiser
Verkoopmanager
Duitsland,
Theben AG

de crux van KNX Data Secure. Theben voorziet met onmiddellijke ingang alle MIX2-actoren van KNX Data Secure. Zelfs meer dan 10 jaar oude modules kunnen worden aangepast. „Je zou kunnen zeggen dat MIX2 al tien jaar Data Secure ready is”, zegt Axel Kaiser, verkoopmanager voor Duitsland en marketingmanager bij Theben, met een knipoog. Tegelijkertijd onderstreept hij echter: „Wij laten de klant nog steeds de vrije keus of men Secure al of niet wil gebruiken. Qua prijs is dat geen verschil en het extra werk is ook zeer gering. Men moet zich echter wel aanpassen aan andere processen. Dat willen we niemand opdringen.”

Het systeem biedt in totaal 129 combinatiemogelijkheden. De uitbreidingsmodules blijven daarbij ongewijzigd, omdat ze via een interne, in eigen beheer ontwikkelde bus met de basismodule communiceren. Axel Kaiser wijst op de voordelen: „Van elk type is er een basis- en een uitbreidingsmodule. Deze flexibiliteit biedt grote voordelen bij het ontwerp. Je hebt altijd uitgangen voor het schakelen, dimmen of aansturen van verwarming en jaloezieën nodig, maar je weet nooit precies hoeveel. Met ons systeem kun je nog tijdens de installatie gewenste wijzigingen aanbrengen.” Dat is zelfs nog na ingebruikname mogelijk zolang er plaats is voor een uitbreidingsmodule.

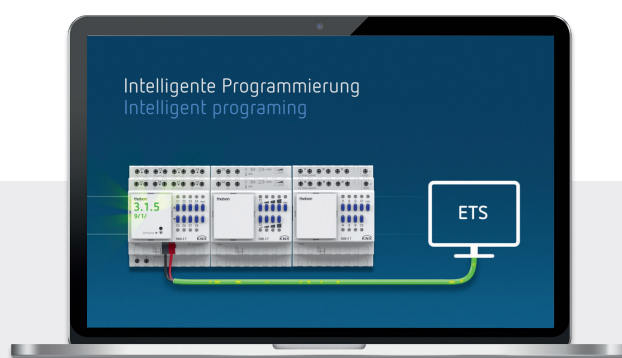
Data Secure in de praktijk

Zoals door Axel Kaiser beschreven, zijn de Secure-modules niet duurder dan de varianten zonder deze functie. Het belangrijkste is de installatie. Het extra werk is echter zeer gering. Michael Saile: „Op elk product is een QR-code aangebracht. Die hoeft je alleen te scannen en daaraan eenmalig een projectwachtwoord toe kennen. De rest doet de ETS automatisch. De code wordt ook apart op een kaart meegeleverd, waarop men de montageplaats kan noteren. Zo kan men de apparaten tijdens de installatie of onafhankelijk daarvan op het bureau registreren.” Zelfs gemengd gebruik is mogelijk, vult Saile aan: „Wanneer een apparaat niet secure is, communiceert niet de hele lijn unsecure, maar worden alleen de telegrammen van dit apparaat niet secure verzonden. Alle andere telegrammen die dit apparaat nodig heeft, kunnen worden versleuteld. Een secure-apparaat kan ook altijd met een unsecure-deelnemer communiceren; het telegram is dan natuurlijk niet versleuteld. Ook dat doet ETS automatisch.” Zo kan ook een bestaande installatie naderhand worden aangepast en ten minste gedeeltelijk beter tegen aanvallen worden beschermd. Zelfs het gebruik van absoluut vereiste speciale componenten is mogelijk, die echter niet met Data Secure verkrijgbaar zijn. De installatie blijft desondanks goed beveiligd.

Theben adviseert het via de QR-code in de ETS geregistreerde apparaat op de juiste plaats te monteren. Belangrijk is dan dat het apparaat dan ook op de eerder bepaalde plaats wordt gemonteerd. Dit kan ook door een installateur zonder KNX kennis worden uitgevoerd. Na de organisatorische integratie is het extra werk van KNX Secure bijna nul, wat echter een zeer overtuigend verkoopargument is.



MIX2-actoren – de video
Intelligent, flexibel, uitbreidbaar



Het MIX2-concept

Zoals bij alle andere producten hecht Theben ook bij MIX2 grote waarde aan een veilige investering. Het systeem is zelfs compatible met de nog oudere MIX1-uitbreidingsmodules. Nauwelijks een ander verkrijgbaar product biedt dezelfde rentabiliteit en flexibiliteit als MIX2. Bovendien kunnen de apparaten zonder programmering worden vervangen. En bij een defect moet alleen de betreffende module, en niet het hele apparaat, worden vervangen. De update van de firmware vindt heel eenvoudig met de ETS-app plaats.

Het vermogen van de afzonderlijke modules voldoet ook aan hoge eisen. Zo kunnen maximaal 24 schakel- of 12 jaloeziekanalen met slechts één busdeelnemer worden gerealiseerd. Schakel-, dim-, jaloezie- en verwarmingsactoren alsmede binaire ingangen kunnen vrij worden gecombineerd. De hieronder beschreven bouwstenen zijn zowel als basis- als uitbreidingsmodule verkrijgbaar, waarbij een basismodule met twee willekeurige uitbreidingsmodules kan worden gecombineerd.

Met deze verscheidenheid aan modules en het optionele gebruik van KNX Data Secure biedt Theben een van de meest flexibele en duurzame actoroplossingen aan. De compatibiliteit met maximaal twintig jaar oude uitbreidingsmodules en de integratie van de nieuwste KNX-standaarden spreken voor zich.

Overzicht van de MIX2-voordelen

#01 Veilig upgraden - ook voor oude in- stallaties

Dankzij de verwijderbare buskoppeling kunnen ook bestaande installaties eenvoudig, snel en voordelig naar KNX Data Secure worden geüpgraded. Vervang de bestaande buskoppeling gewoon door de nieuwe.

#02 Voordelige uitbreidingsappara- ten

Omdat alleen het basisapparaat met een buskoppeling is uitgerust, worden de kosten voor de uitbreidingsapparaten (E) en door de bespaarde systeemapparaten tot een derde verlaagd. Dat is zeker de moeite waard. Vooral in de projectbouw. Reken het zelf maar uit!

#03 Flexibel uitbreidbaar

Verlichten, dimmen, verwarmen, klimaat of de zonwering regelen is met de KNX MIX2 niet alleen geen probleem, maar aanbevelenswaardig. Zo maakt u met MIX2 een individuele, op elke ruimte en de behoeften daarvan afgestemde oplossing. Deze flexibiliteit vindt u zo alleen bij Theben.

#04 Overzichtelijke applicatie

De configuratiemenu's in de ETS zijn niet alleen via alle actoren identiek gestructureerd, maar ook zeer overzichtelijk en intuïtief vormgegeven. Afhankelijk van het project en de eisen kunnen de gewenste actoren via dropdown-menu's worden geselecteerd. Ook naderhand wanneer een uitbreidingsmodule met andere functies nodig is. Dat is zo alleen bij Theben mogelijk.

De mix zorgt ervoor KNX MIX2-actoren Compleet, flexibel, uitbreidbaar



Schakelactoren

Voor standaardfuncties zijn een 4-voudige en een 8-voudige schakelactor verkrijgbaar. Deze bieden een LED-schakelvermogen van max. 600 W bij een maximale inschakelstroom van 800 A bij 200 μ s.

Moet de werking van een apparaat worden bewaakt, dan is een 4-voudige schakelactor met geïntegreerde stroommeting een prima keuze. Deze kan bijvoorbeeld de uitval van de verlichting op een veiligheidsrelevante plaats zoals in een trappenhuis worden gedetecteerd. De module heeft een LED-schakelvermogen van max. 850 W bij een maximale inschakelstroom van 1500 A bij 200 μ s. Een schakel-/jaloezieactor 8/4-voudig vult het assortiment schakelactoren aan.

Basisapparaten

- RMG 8 S KNX (artikelnr. 4930220)
- RMG 4 U KNX (artikelnr. 4930223)
- RMG 4 I KNX (artikelnr. 4930210)
- RMG 8 T KNX (artikelnr. 4930200)

Uitbreidingsapparaten

- RME 8 S KNX (artikelnr. 4930225)
- RME 4 U KNX (artikelnr. 4930228)
- RME 4 I KNX (artikelnr. 4930215)
- RME 8 T KNX (artikelnr. 4930205)



Dimactor

De 2-voudige dimactor werkt bijna probleemloos met bijna elke verkrijgbare LED-lamp. Daardoor is deze ideaal voor retrofit-toepassingen. Met max. 400 W LED-vermogen per kanaal en 800 W bij parallel gebruik is deze zelfs geschikt voor grotere verlichtingsinstallaties.

- DMG 2 T KNX (artikelnr. 4930270)
- DME 2 T KNX (artikelnr. 4930275)



Jaloezieactoren

Twee 4-voudige jaloezieactoren voor 230V, resp. 24V bedrijfsspanning bieden omvangrijke zonweringsfuncties. De looptijden kunnen op andere kanalen worden overgedragen.

- JMG 4 T KNX (artikelnr. 4930250)
- JME 4 T KNX (artikelnr. 4930255)
- JMG 4 T 24V KNX (artikelnr. 4930260)
- JME 4 T 24V KNX (artikelnr. 4930265)



Verwarmingsactor

Universeel voor 24 – 230V AC kan de 6-voudige verwarmingsactor worden gebruikt. Deze is uitgerust met een geïntegreerde regelaar voor verwarmen en koelen in elk kanaal.

- HMG 6 T KNX (artikelnr. 4930240)
- HME 6 T KNX (artikelnr. 4930245)



Binaire ingang

Een 6-voudige binaire-ingangsmodule rondt het productassortiment af. De meervoudige spanningsingangen zijn geschikt voor 10-230V AC/DC. Via een geïntegreerde netadapter kunnen de ingangen van stroom worden voorzien.

- BMG 6 T KNX (artikelnr. 4930230)
- BME 6 T KNX (artikelnr. 4930235)

