0273-1-**8768** | 12.04.2016

Cyber Security
Disclaimer for Products

Bitte wählen Sie eine Sprache aus. / Please choose a language. / Vælg et sprog. / Por favor, seleccione un idioma. / Veuillez sélectionner une langue. / Valitse kieli. / Επιλέξτε μια γλώσσα. / Selezionare una lingua. / Kies een taal a.u.b. / Velg språk. / Proszę wybrać język. / Por favor selecione uma língua / Выберите язык. / Välj ett språk. /请选择语言 。/ Vyberte prosím jazyk. / Lütfen bir dil seçin.

CN	中文	**CZ**	**Česky**
DE	**Deutsch**	**DK**	**Dansk**
EN	**English**	**ES**	**Español**
FR	**Français**	**FI**	**Suomi**
GR	**Ελληνικά**	**IT**	**Italiano**
NL	**Netherlands**	**NO**	**Norsk**
PL	**Polski**	**PO**	**Português**
RU	**Русский**	**SE**	**Svenska**
TR	**Türkçe**		

Cyber Security
Disclaimer for Products

Die Branche ist verstärkt mit Internetsicherheitsrisiken konfrontiert. Um Stabilität, Sicherheit und Robustheit seiner Lösungen zu erhöhen, hat ABB im Rahmen des Produktentwicklungsprozesses offiziell Robustheitsprüfungen zur Internetsicherheit eingeführt.

Die folgenden Hinweise dienen darüberhinaus als Leitfaden und beschreiben Mechanismen, die verwendet werden können um die Sicherheit von KNX / f@h-Anlagen zu verbessern.

Verhindern des Zugangs zu den unterschiedlichen Medien

Die Basis jedes Schutz-Konzeptes bildet die sorgfältige Abschottung des Systems gegen unberechtigten Zugriff. Im Falle einer KNX / f@h-Anlage gilt, dass nur befugte Personen (Installateur, Hausmeister, Nutzer) physischen Zugang zur KNX/f@h-Anlage haben dürfen. Bei der Planung und Installation müssen für jedes KNX/f@h-Medium die kritischen Punkte bestmöglich geschützt werden.
Allgemein gilt, dass Anwendungen und Geräte fest installiert werden sollten, um zu verhindern, dass diese leicht entfernt werden und dadurch unbefugte Personen Zugang zur KNX/f@h-Anlage haben.
Unterverteilungen mit KNX/f@h-Geräten sollten verschlossen sein, oder sich in Räumen befinden, zu denen nur befugte Personen Zugang haben.

Twisted Pair-Verkabelung

- Die Leitungsenden des KNX/f@h Twisted Pair-Kabels sollten nicht sichtbar sein oder aus der Wand herausstehen, weder im noch außerhalb des Gebäudes.
- Wenn verfügbar, sollten die Diebstahlschutzeinrichtungen der Applikationsmodule verwendet werden.
- Busleitungen im Außenbereich stellen ein erhöhtes Risiko dar. Der physische Zugang zum KNX/f@h Twisted Pair-Kabel sollte hier besonders erschwert werden.
- Geräte, die in begrenzt geschützten Bereichen verbaut sind (Außenbereich, Tiefgarage, WC, etc.), können als zusätzlicher Schutz als eigene Linie ausgeführt werden. Durch Aktivierung der Filtertabellen im Linienkoppler (**nur KNX**) wird verhindert, dass ein Angreifer Zugriff auf die gesamte Anlage erlangen kann.

IP-Verkabelung innerhalb des Gebäudes

- Für die Gebäudeautomation sollte ein getrenntes LAN- oder WLAN-Netzwerk mit eigener Hardware (Router, Switches etc.) verwendet werden.
- Unabhängig von der KNX/f@h-Anlage sind unbedingt die üblichen Sicherheitsmechanismen für IP-Netzwerke anzuwenden. Diese sind beispielsweise:
    - MAC-Filter
    - Verschlüsselung von Drahtlosnetzwerken
    - Verwendung starker Passwörter und Schutz dieser vor unbefugten Personen

Anbindung an das Internet

- KNXnet/IP Routing und KNXnet/IP Tunneling nutzen eine unverschlüsselte Datenübertragung und sind daher nicht für Verwendung im öffentlichen Internet vorgesehen. Aus diesem Grund dürfen keine Ports von Routern Richtung Internet geöffnet werden: dies verhindert, dass die KNX/f@h Kommunikation im Internet sichtbar wird.
- Ein Zugriff auf eine Anlage aus dem Internet kann auf folgende Weise ermöglicht werden:
    - Zugang zu KNX/f@h Installationen über VPN Verbindungen: dies setzt jedoch einen Router mit VPN Server-Funktionalität voraus oder einen Server.
    - Verwendung von herstellerspezifischen Lösungen oder Visualisierungen, z.B. mit Zugang über https.

Cyber Security
Disclaimer for Products

Industry faces intensifying cyber security risks. In order to increase stability, security, and robustness in its solutions, ABB has formally established cyber security robustness testing as part of the product development process.

In addition the following information serves as a guide and describes mechanisms which are used to improve the safety of KNX / f@h systems.

Prevention of access to the different media

The careful isolation of the system against unauthorized access is the basis for each protective concept. In case of a KNX / f@h system it is only authorized persons (fitter, caretaker, user) who are allowed physical access to the KNX/f@h system. During planning and installation the critical points must be protected as best as possible for every KNX/f@h medium.
As a general rule, applications and devices should be permanently installed to prevent their easy removal and thereby allow access to unauthorized persons to the KNX / f@h system.
Sub-distributions with KNX/f@h devices are to be locked or located in rooms to which only authorized persons have access.

Twisted pair-cabling

- The cable ends of the KNX/f@h Twisted Pair cable should not be visible or project out from the wall, neither inside nor outside the building.
- If available, the theft protection facilities of the application modules should be used.
- Bus lines in outdoor areas represent an increased risk. Here the physical access to the KNX/f@h Twisted Pair cable should be made exceptionally difficult.
- Devices installed in areas with limited protection (outdoors, underground car parks, WC, etc.) can be designed as independent line for additional protection. The activation of filter charts in the line coupler (**only KNX**) prevents attackers from gaining access to the entire system.

IP-cabling within the building

- For building automation a separate LAN or WLAN network with its own hardware (router, switches, etc.) should be used.
- It is absolutely essential that the normal safety mechanisms for IP networks are used independent from the KNX/f@h system. These are, for example:
    - MAC filter
    - Encryption of wireless networks
    - Use of complex passwords and protection of these against unauthorized persons.

Internet

- KNXnet/IP routing and KNXnet/IP tunnelling use data transmission without encryption and are not intended for use with the Internet. For this reason no ports of routers are to be opened in the direction of the Internet: this prevents KNX/f@h communication from becoming visible on the Internet.
- Access to a system from the Internet is possible with the following method:
    - Access to the KNX/f@h installations via VPN connections: this, however, requires a router with VPN server function or a server.
    - Use of manufacturer-specific solutions or visualizations, e.g. with access via https.

Cyber Security
Disclaimer for Products

Branchen er i stigende grad udfordret af sikkerhedsrisici på internettet. For at forbedre stabiliteten, sikkerheden og robustheden i sine løsninger har ABB som led i produktudviklingsprocessen officielt indført robusthedstests i forhold til internetsikkerheden.

De følgende henvisninger er derudover en vejledning, der beskriver de mekanismer, der kan anvendes til at forbedre sikkerheden ved KNX / f@h-anlæg.

Forhindring af adgang til de forskellige medier

Kernen i ethvert sikkerhedskoncept er at sikre systemet omhyggeligt mod uvedkommende adgang. Ved et KNX / f@h-anlæg gælder det, at kun autoriserede personer (installatør, opsynsmand, bruger) må have fysisk adgang til KNX/f@h-anlægget. I forbindelse med planlægningen og installationen skal de kritiske punkter for hvert KNX/f@h-medie beskyttes bedst muligt.
Generelt gælder det, at applikationer og enheder bør installeres fast for at forhindre, at de er lette at fjerne og dermed kan give uvedkommende personer adgang til KNX/f@h-anlægget.
Viderefordelinger med KNX/f@h-enheder bør være aflåst eller kun findes i rum, som autoriserede personer har adgang til.

Twisted Pair-kabelføring

- Ledningsenderne på KNX/f@h Twisted Pair-kablet bør ikke være synlige eller stikke ud af væggen, hverken inde i eller uden for bygningen.
- Eventuelle tyverisikringsanordninger til applikationsmodulerne bør anvendes.
- En særlig risiko udgør udendørs busledninger. Her er det særligt vigtigt, at den fysiske adgang til KNX/f@h Twisted Pair-kablet er vanskeliggjort.
- Enheder, der er monteret i områder med begrænset beskyttelse (udendørsområder, parkeringskældre, toiletter, etc.), kan som ekstra beskyttelse udføres som egen linje. Ved at aktivere filtertabellerne i linjekobleren (**kun KNX**) forhindres uvedkommende adgang til hele anlægget.

IP-kabelføring i bygningen

- Til bygningsautomatikken bør der anvendes et adskilt LAN- eller WLAN-netværk med selvstændig hardware (router, switches, etc.).
- Uafhængigt af KNX/f@h-anlægget bør de generelle sikkerhedsmekanismer til IP-netværk altid anvendes. Disse er f.eks.:
    - MAC-filter
    - Kryptering af trådløse netværk
    - Anvendelse af stærke passwords og hindring af uvedkommendes adgang til disse

Forbindelse til internettet

- KNXnet/IP routing og KNXnet/IP tunneling benytter en ukrypteret dataoverførsel og er derfor ikke beregnet til brug på det offentlige internet. Derfor må ingen routerporte i retning mod internettet åbnes: Dette forhindrer, at KNX/f@h-kommunikationen på internettet bliver synlig.
- Adgang til et anlæg via internettet kan muliggøres på følgende måde:
    - Adgang til KNX/f@h installationer via VPN-forbindelser: Dette forudsætter dog en router med VPN-server-funktionalitet eller en server.
    - Anvendelse af producentspecifikke løsninger eller visualiseringer, f.eks. med adgang via https.

Cyber Security
Disclaimer for Products

El sector se enfrenta en Internet a riesgos para la seguridad cada vez mayores. ABB ha introducido oficialmente ensayos de robustez, dentro del proceso de desarrollo de los productos, para aumentar la estabilidad, la seguridad y la robustez de sus soluciones.

Las siguientes indicaciones sirven también de guía y describen los mecanismos que pueden emplearse para mejorar la seguridad de las instalaciones KNX/f@h.

Denegación de acceso a los diferentes medios

La base de cualquier concepto de seguridad establece una protección minuciosa del sistema frente al acceso no autorizado. En el caso de una
instalación KNX/f@h se considera que solo las personas autorizadas (instalador, conserje, usuario) deben poseer acceso físico a una instalación KNX/f@h. Para la planificación e instalación de cualquier medio KNX/f@h se deben proteger los puntos críticos de la mejor manera posible.
En general, se considera que las aplicaciones y los aparatos se deben instalar de manera fija para evitar que estos puedan ser fácilmente retirados, lo que permitiría el acceso a personas no autorizadas a las instalaciones KNX/f@h.
Las subdistribuciones con aparatos KNX/f@h deben permanecer cerradas o encontrase en estancias a las que solamente tengan acceso las personas autorizadas.

Cableado de par trenzado

- Los terminales de los cables KNX/f@h de par trenzado no deben estar visibles ni sobresalir de la pared, así como tampoco deben estar accesibles desde el exterior del edificio.
- De estar disponibles, se deben emplear los dispositivos de protección antirrobo de los módulos de aplicación.
- Los cables de bus colocados en el exterior representan un gran riesgo. En este caso, se debe obstaculizar especialmente el acceso físico a los cables KNX/f@h de par trenzado.
- Los aparatos instalados en áreas con una cierta protección limitada (zonas exteriores, garajes subterráneos, aseos, etc.) se pueden ejecutar en forma de línea individual como protección adicional. Mediante la activación de las tablas de filtros del acoplador de línea (**solo KNX**), se evita que un atacante pueda acceder a toda la instalación.

Cableado IP dentro del edificio

- Para la automatización del edificio se debe emplear una red LAN o WiFi independientes con su propio hardware (router, switches, etc.).
- Independientemente de la instalación KNX/f@h, se deben aplicar necesariamente los mecanismos generales de seguridad para redes IP. Estos son, por ejemplo:
    - Filtros MAC
    - Cifrado de redes inalámbricas
    - Utilización de claves de acceso fuertes y protección de las mismas frente a personas no autorizadas.

Conexión a Internet

- KNXnet/IP Routing y KNXnet/IP Tunneling emplean una transmisión de datos sin cifrado, por lo que no están previstas para ser utilizadas en redes públicas de Internet. Por esta razón, no debe abrirse ningún puerto del router hacia Internet: con esto se evita que la comunicación KNX/f@h sea visible desde Internet.
- El acceso a una instalación desde Internet se puede efectuar de la siguiente manera:
    - Acceso a las instalaciones KNX/f@h mediante conexiones VPN: esto presupone contar con un router con funcionalidad de servidor VPN o con un servidor.
    - Utilización de soluciones o visualizaciones específicas del fabricante, por ejemplo con acceso mediante https.

Cyber Security
Disclaimer for Products

La branche se voit de plus en plus confrontée aux risques de sécurité Internet. Afin d'améliorer la stabilité, la sécurité et la robustesse de ses solutions, ABB a introduit officiellement des essais de robustesse en matière de sécurité Internet, dans le cadre de son processus de développement de produits.

De plus, les informations mentionnées ci-dessous font fonction de guide et décrivent les moyens qui peuvent être utilisés afin d'améliorer la sécurité des installations KNX/f@h.

Empêcher l'accès aux différents moyens

La base de tout concept de protection est d'isoler le système complètement afin de bloquer tout accès non autorisé. Dans le cas d'une
installation KNX/f@h, seules les personnes autorisées (installateurs, gardiens, utilisateurs) doivent pouvoir avoir un accès physique à une telle installation. Lors de la planification et de l'installation, les endroits critiques doivent être protégés au mieux pour chacun des moyens KNX/f@h.
En règle générale, les applications et les appareils doivent être fixes afin d'empêcher qu'ils ne puissent être retirés facilement et, par conséquent, permettre un accès à l'installation KNX/f@h à des personnes non autorisées.
En cas de dérivation, les appareils KNX/f@h doivent être sous clé ou installés dans des locaux uniquement accessibles aux personnes qui y sont autorisées.

Câblage Twisted Pair

- Les extrémités du câble Twisted Pair KNX/f@h ne doivent pas être visibles ou dépassées du mur, ni à l'intérieur ni à l'extérieur du bâtiment.
- Si disponibles, utilisez les dispositifs antivol des modules d'application.
- Les lignes de bus installées à l'extérieur représentent un plus grand risque. Dans ce cas, il est nécessaire qu'un accès physique au câble Twisted Pair KNX/f@h soit particulièrement difficile.
- Les appareils situés dans des zones peu protégées (extérieurs, parking souterrain, WC, etc.) peuvent être installés avec une ligne qui leur est réservée afin qu'ils soient davantage protégés. En activant les tables de filtrage dans le coupleur de lignes (**uniquement pour KNX**), il est possible, en cas d'intrusion, d'éviter que la personne ait accès à l'ensemble de l'installation.

Câblage IP dans le bâtiment

- Au niveau de l'immotique, installez un réseau local ou Wi-Fi avec un matériel à part (routeur, switchs, etc.).
- Indépendamment de l'installation KNX/f@h, utilisez impérativement les moyens courants de sécurité destinés aux réseaux IP. Ce sont par exemple :
    - Filtrage MAC
    - Cryptage des réseaux sans fil
    - Utilisation de mots de passe forts en les protégeant contre toute personne non autorisée

Connexion à l'Internet

- Le routage KNXnet/IP et les tunnels KNXnet/IP utilisent une transmission de données non chiffrée et ne sont donc pas prévus pour une utilisation dans l'Internet public. C'est la raison pour laquelle aucun port des routeurs ne doit être ouvert pour l'Internet : cela empêche que les communications KNX/f@h ne puissent être lues sur Internet.
- Un accès à une installation à partir de l'Internet peut être rendu possible de la manière suivante :
    - Accès des installations KNX/f@h via une connexion VPN : dans ce cas, il est cependant nécessaire d'avoir un routeur avec les fonctions d'un serveur VPN ou un serveur.
    - Utilisation de solutions spécifiques au fabricant ou visualisations, par exemple, avec un accès via https.

Cyber Security
Disclaimer for Products

Alalla ilmenee yhä enemmän internet-turvallisuuteen vaikuttavia riskejä. ABB on kehittänyt tuotekehitysprosessinsa puitteissa internet-turvallisuuden tarkastamiseen käytettäviä virallisia luotettavuustarkastuksia eri ratkaisujen luotettavuuden ja turvallisuuden varmistamiseksi.

Myös seuraavat tiedot ovat ohjeita ja niissä kuvataan mekanismeja, joita voidaan käyttää KNX/f@h-järjestelmien turvallisuuden parantamiseksi.

Eri välineisiin pääsyn estäminen

Kaikki suojakonseptit perustuvat järjestelmän huolelliseen suojaamiseen asiattomalta pääsyltä. Kun kyseessä on KNX/f@h-järjestelmä, vain asianmukaiset oikeudet omaavilla henkilöillä (asentajat, talonmiehet, käyttäjät) saa olla fyysinen pääsy KNX/f@h-järjestelmään.

Suunnittelun ja asennuksen yhteydessä jokaisen KNX/f@h-välineen kriittiset kohdat on suojattava parhaalla mahdollisella tavalla. Sovellukset ja laitteet tulee yleisesti ottaen asentaa kiinteästi, jotta vältetään niiden helppo poistaminen ja siten asiattomien henkilöiden pääsy KNX/f@h-järjestelmään.

KNX/f@h-laitteiden alajaot tulee lukita tai ne on sijoitettava tiloihin, joihin vain valtuutetuilla henkilöillä on pääsy.

Twisted Pair-kaapelointi

- KNX/f@h-järjestelmän Twisted Pair -kaapeleita ei saa jättää näkyviin, ei seinässä eikä rakennuksen ulkopuolella.
- Sovellusmoduulien varkaussuojalaitteita on käytettävä, mikäli ne ovat saatavilla.
- Ulkona sijaitsevat väyläjohdot aiheuttavat kohonneen riskin. Fyysinen pääsy KNX/f@h-järjestelmän Twisted Pair -kaapeleihin tulee tehdä mahdollisimman vaikeaksi.
- Rajoitetusti suojatuille alueille (ulkotilat, maanalainen autotalli, WE jne.) sijoitetut laitteet voi kytkeä lisäsuojatoimenpiteenä omaksi linjaksi. Aktivoimalla suodatintaulukot linjakytkimestä (**vain KNX**) estetään asiattomien henkilöiden pääsy koko järjestelmään.

IP-kaapelointi rakennuksen sisällä

- Rakennusautomaatiota varten tulee käyttää erillistä LAN- tai WLAN-verkkoa, jossa on oma järjestelmä (reititin, kytkimet, jne.).
- KNX/f@h-järjestelmästä riippumatta on ehdottomasti huolehdittava myös muista tarvittavista IP-verkon turvamekanismeista. Niitä ovat esimerkiksi:
    - MAC-suodattimet
    - Langattomien verkkojen salaus
    - Vahvojen salasanojen käyttö ja niiden suojaaminen asiattomilta henkilöiltä

Yhteys internetiin

- KNXnet/IP Routing ja KNXnet/IP Tunneling käyttävät suojaamatonta tiedonsiirtoa eivätkä ne sovi siitä syystä internet-käyttöön. Siksi reititinten portteja ei saa avata internetille. Siten estetään KNX/f@h-tiedonsiirron näkyminen internetissä.
- Pääsy laitteeseen internetistä voidaan mahdollistaa seuraavalla tavalla:
    - Pääsy KNX/f@h-asennuksiin VPN-yhteyksien kautta. Edellytyksenä on kuitenkin VPN-palvelintominnolla varustettu reititin tai palvelin.
    - Valmistajakohtaisten ratkaisujen tai visualisointien käyttö, esim. pääsy https:n kautta.

Cyber Security
Disclaimer for Products

Ο κλάδος αντιμετωπίζει έντονα κίνδυνους ασφάλειας που σχετίζονται με Internet. Προκειμένου να αυξηθεί η σταθερότητα, η ασφάλεια και η αξιοπιστία των λύσεών της, η ABB εισήγαγε επισήμως στα πλαίσια της διαδικασίας ανάπτυξης προϊόντων ελέγχους αξιοπιστίας για την ασφάλεια Internet.

Οι παρακάτω υποδείξεις εξυπηρετούν επίσης ως κατευθυντήριες οδηγίες και περιγράφουν μηχανισμούς, οι οποίοι μπορούν να χρησιμοποιηθούν για τη βελτίωση εγκαταστάσεων KNX / f@h.

Παρεμπόδιση πρόσβασης σε διάφορα μέσα

Η βάση κάθε μεθόδου προστασίας διαμορφώνει μια προσεκτική περιχαράκωση του συστήματος έναντι μη εξουσιοδοτημένης πρόσβασης. Στην περίπτωση μιας εγκατάστασης KNX / f@h ισχύει ότι μόνο εξουσιοδοτημένα άτομα (εγκαταστάτης, επιστάτης, χρήστης) επιτρέπεται να έχουν φυσική πρόσβαση στην εγκατάσταση KNX/f@h.

Κατά το σχεδιασμό και την εγκατάσταση πρέπει να προστατεύονται κατά το δυνατόν καλύτερα για κάθε μέσο KNX/f@h τα κρίσιμα σημεία.

Γενικά η εγκατάσταση των εφαρμογών και των συσκευών θα πρέπει να είναι σταθερή, ώστε να αποφεύγεται η εύκολη απομάκρυνσή τους και συνεπώς η πρόσβαση μη εξουσιοδοτημένων ατόμων στην εγκατάσταση KNX/f@h.

Υποδιανομές με συσκευές KNX/f@h θα πρέπει να είναι κλειδωμένες ή να βρίσκονται σε χώρους στους οποίους έχουν πρόσβαση μόνο εξουσιοδοτημένα άτομα.

Καλωδίωση συνεστραμμένου ζεύγους

- Τα άκρα του καλωδίου συνεστραμμένου ζεύγους KNX/f@h δεν πρέπει να είναι ορατά ή να προεξέχουν από τον τοίχο, ούτε στο εξωτερικό του κτιρίου.
- Εφόσον υπάρχουν, θα πρέπει να χρησιμοποιούνται οι αντικλεπτικές διατάξεις των μονάδων εφαρμογής.
- Αγωγοί διαύλου στον εξωτερικό χώρο αποτελούν αυξημένο κίνδυνο. Η φυσική πρόσβαση στο καλώδιο συνεστραμμένου ζεύγους KNX/f@h θα πρέπει εδώ να είναι ιδιαίτερα δύσκολη.
- Συσκευές οι οποίες είναι τοποθετημένες σε ελάχιστα προστατευμένους χώρους (έξω, υπόγειο γκαράζ, WC, κ.λπ.), μπορούν ως έξτρα προστασία να έχουν ξεχωριστή γραμμή. Με την ενεργοποίηση των πινάκων φίλτρων στο συζευκτήρα γραμμών (**μόνο KNX**) παρεμποδίζεται η πρόσβαση επιτηδείων σε ολόκληρη την εγκατάσταση.

Καλωδίωση IP εντός του κτιρίου

- Για την αυτοματοποίηση του κτιρίου θα πρέπει να χρησιμοποιείται ένα ξεχωριστό δίκτυο LAN ή WLAN με ξεχωριστό υλικό (δρομολογητής, μεταγωγείς κ.λπ.).
- Ανεξάρτητα από την εγκατάσταση KNX/f@h θα πρέπει να χρησιμοποιηθούν οπωσδήποτε οι τυπικοί μηχανισμοί ασφαλείας για δίκτυο IP. Αυτά είναι λόγου χάρη:
    - Φίλτρα MAC
    - Κρυπτογράφηση ασύρματων δικτύων
    - Χρήση ισχυρών κωδικών ασφαλείας και προστασία τους από μη εξουσιοδοτημένα άτομα

Σύνδεση στο Internet

- Οι διαδικασίες KNXnet/IP Routing και KNXnet/IP Tunneling χρησιμοποιούν μη κωδικοποιημένη μετάδοση δεδομένων και συνεπώς δεν προβλέπονται για χρήση στο Internet. Για το λόγο αυτόν δεν πρέπει να ανοίγουν θύρες δρομολογητή για Internet: έτσι δεν μπορεί να γίνει ορατή η επικοινωνία του KNX/f@h στο Internet.
- Μια πρόσβαση σε μια εγκατάσταση από το Internet μπορεί να γίνει με τους παρακάτω τρόπους:
    - Πρόσβαση σε εγκαταστάσεις KNX/f@h μέσω συνδέσεων VPN: αυτό προϋποθέτει ωστόσο δρομολογητή με λειτουργία διακομιστή VPN ή διακομιστή.
    - Χρήση λύσεων ή οπτικών βοηθημάτων του κατασκευαστή, π.χ. με πρόσβαση μέσω https.

Cyber Security
Disclaimer for Products

Il settore si trova sempre più spesso a dover affrontare rischi legati alla sicurezza in Internet. Per aumentare la stabilità, la sicurezza e la robustezza delle sue soluzioni, ABB ha ufficialmente introdotto verifiche della robustezza per la sicurezza in Internet nell'ambito del processo di sviluppo dei prodotti.

Le seguenti indicazioni servono inoltre da linee guida e descrivono i meccanismi utilizzabili per migliorare la sicurezza di impianti KNX / f@h.

Impedire l'accesso ai diversi mezzi di comunicazione

La base di qualsiasi piano per la sicurezza è costituita da un accurato isolamento del sistema contro accessi non autorizzati. Nel caso di un
impianto KNX / f@h, l'accesso fisico allo stesso è consentito solamente a persone autorizzate (installatore, portiere, utilizzatore). Nel corso della progettazione e dell'installazione, vanno protetti nel miglior modo possibile i punti critici per ciascun mezzo di comunicazione KNX/f@h.
In generale, applicazioni e apparecchi andrebbero installati in modo permanente per impedire che siano facili da rimuovere consentendo di conseguenza l'accesso agli impianti KNX/f@h a persone non autorizzate.
Distribuzioni secondarie con apparecchi KNX/f@h dovrebbero essere chiuse oppure trovarsi in ambienti accessibili esclusivamente a persone autorizzate.

Cablaggio Twisted Pair

- Le estremità del cavo Twisted Pair KNX/f@h non dovrebbero essere visibili o fuoriuscire dalla parete, né al di fuori né all'interno dell'edificio.
- Laddove disponibili, andrebbero utilizzati i dispositivi antifurto dei moduli applicativi.
- Collocare i cavi bus nelle zone esterne è più rischioso. L'accesso fisico al cavo Twisted Pair KNX/f@h dovrebbe essere reso in questo caso il più complicato possibile.
- Apparecchi installati in ambienti poco protetti (ambienti esterni, parcheggi sotterranei, WC, ecc.), ai fini di un'ulteriore protezione possono essere strutturati come linea individuale. Attivando le tabelle di filtro all'interno dell'accoppiatore di linea (**solamente KNX**), si impedisce ai malintenzionati l'accesso all'intero impianto.

Cablaggio IP all'interno dell'edificio

- Per l'automazione dell'edificio andrebbe utilizzata una rete LAN o WLAN separata con un proprio hardware (router, interruttori, ecc.).
- Indipendentemente dall'impianto KNX/f@h è assolutamente necessario adottare i consueti meccanismi di sicurezza per reti IP. Ad esempio:
    - Filtro MAC
    - Criptaggio di reti wireless
    - Utilizzo di password forti e relativa protezione da persone non autorizzate

Collegamento a Internet

- Il routing KNXnet/IP e il tunneling KNXnet/IP utilizzano una trasmissione dati non codificata, pertanto non sono previsti per l'uso nella rete Internet pubblica. Per questa ragione non possono essere aperte porte dei router per la connessione a internet: in questo modo si impedisce la visibilità in internet della comunicazione KNX/f@h.
- L'accesso ad un impianto da Internet può essere consentito nel seguente modo:
    - Accesso a installazioni KNX/f@ tramite connessioni VPN: ciò presuppone tuttavia un router con funzione server VPN oppure un server.
    - Utilizzo di soluzioni specifiche del produttore oppure visualizzazioni, per es. con accesso tramite http.

Cyber Security
Disclaimer for Products

De branche wordt in toenemende mate geconfronteerd met internetveiligheidsrisico's. Om de stabiliteit, veiligheid en robuustheid van onze oplossingen te verhogen, heeft ABB in het kader van het productontwikkelingsproces officieel robuustheidstest voor internetveiligheid ingevoerd.

Bovendien geven we met volgende aanwijzingen richtsnoeren en beschrijven mechanismen die gebruikt kunnen worden om de veiligheid van KNX / f@h-installaties te verbeteren.

De toegang tot de verschillende media verhinderen

De basis van ieder beveiligingsconcept vormt de zorgvuldige bescherming van het systeem tegen onbevoegde toegang. Bij een KNX / f@h-installatie betekent dat uitsluitend bevoegde personen (installateur, huismeester, gebruiker) fysieke toegang tot de KNX/f@h-installatie mag hebben. Bij planning en installatie moet voor ieder KNX/f@h-medium de kritische punten zo goed mogelijk worden beschermd.
In het algemeen geldt dat toepassingen en apparaten vast moeten worden geïnstalleerd om te voorkomen dat deze gemakkelijk kunnen worden verwijderd waardoor onbevoegde personen toegang krijgen tot de KNX/f@h-installatie.
Onderverdelingen met KNX/f@h-apparaten moeten afgesloten zijn of zich in ruimtes bevinden waartoe onbevoegde personen geen toegang hebben.

Twisted Pair-bedrading

- De kabeleinden van de KNX/f@h Twisted Pair-kabel mogen zowel binnen als buiten het gebouw niet zichtbaar zijn of uit de muur steken.
- Indien beschikbaar moeten de diefstalbeschermingsvoorzieningen van de applicatiemodules worden gebruikt.
- Buskabels buiten vormen een verhoogd risico. Hier moet vooral de fysieke toegang tot de KNX/f@h Twisted Pair-kabel worden bemoeilijkt.
- Apparaten die op beperkt beschermde locaties zijn gebouwd (buiten, parkeergarage, wc ect.) kunnen als extra beveiliging als eigen lijn worden uitgevoerd. Met de activering van de filtertabellen in de lijnkoppelaar (**alleen KNX**) wordt voorkomen dat een aanvaller toegang tot de gehele installatie kan krijgen.

IP-bedrading binnen het gebouw

- Voor de gebouwautomatisering moet een gescheiden LAN- of WLAN-netwerk met eigen hardware (router, switches etc.) worden gebruikt.
- Onafhankelijk van de KNX/f@h-installatie moeten altijd de gebruikelijke veiligheidsmechanismen voor IP-netwerken worden gebruikt. Deze zijn bijvoorbeeld:
    - MAC-filter
    - versleuteling van draadloze netwerken
    - gebruik van sterke wachtwoorden en bescherming ervan tegen onbevoegde personen

Internetverbinding

- KNXnet/IP-routing en KNXnet/IP-tunneling gebruiken een onversleutelde gegevensoverdracht en zijn daarom niet bedoeld voor gebruik op het openbare internet. Om deze reden mogen geen poorten van routers richting internet worden geopend: dit voorkomt dat de KNX/f@h-communicatie op internet zichtbaar wordt.
- Op de volgende wijze is de installatie toegankelijk via het internet:
    - Toegang tot KNX/f@h-installaties via VPN-verbindingen: dit veronderstelt echter een router met VPN-serverfunctionaliteit of een server.
    - Gebruik van fabrikantspecifieke oplossingen of visualiseringen, bijvoorbeeld toegang via https.

Cyber Security
Disclaimer for Products

Bransjen er sterkere konfrontert med internettsikkerhetsrisikoer. For å øke stabiliteten, sikkerheten og robustheten til løsningene sine har ABB i produktutviklingsprosessen offisielt innført robusthetskontroller for å oppnå internettsikkerhet.

De følgende anvisningene fungerer i tillegg som ledetråder, og beskriver mekanismer som kan brukes for å øke sikkerheten til KNX / f@h-anlegg.

Forhindrer tilgang til forskjellige medier

Grunnlaget i ethvert sikkerhetskonsept er basert på at det bygges brannmurer mellom systemene for å hindre uautorisert tilgang.
For
KNX / f@h-anlegg gjelder at kun autorisert personell (installatør, vaktmester, bruker) skal ha fysisk tilgang til KNX/f@h-anlegg. Ved prosjektering og installasjon må de kritiske punktene for hvert KNX/f@h-medium beskyttes best mulig.
Generelt gjelder at anvendelser og apparater fastmonteres skal fastmonteres for å forhindre at disse er lette å fjerne, og dermed sikre at ikke-autoriserte personer får tilgang til KNX/f@h-anlegget.
Underfordelinger med KNX/f@h-apparater skal være låst eller befinne seg i rom hvor kun autorisert personell har tilgang.

Twisted Pair-kabling

- Ledningsendene på Twisted Pair-kabler i KNX/f@h skal ikke være synlig eller stikke ut av veggen, og spesielt ikke utenfor bygninger.
- Hvis mulig skal man tyveribeskytte applikasjonsmoduler.
- Bussledninger utendørs representerer økt risiko. Den fysiske tilgangen til KNX/f@h Twisted Pair-kabelen skal her gjøres spesielt vanskelig tilgjengelig.
- Apparater som er montert i området med begrenset beskyttelse (utendørs, garasjeanlegg, WC etc.) kan beskyttes ekstra ved å koble dem til en separat linje. Ved å aktivere filtertabellen i linjekobleren (**kun KNX**), forhindrer man at en angriper får tilgang til hele anlegget.

IP-kabling i bygningen

- For bygningsautomasjon skal man bruke et adskilt LAN-eller WLAN-nettverk med egen maskinvare (router, svitsjer etc.).
- Uavhengig av KNX/f@h-anlegget skal man alltid benytte sikkerhetsmekanismene i IP-nettverket. Dette er f.eks.:
    - MAC-filter
    - Krypterin av trådløse nettverk
    - Pruke sterke passord og beskyttelse mot uautorisert personell

Tilkobling til internett

- KNXnet/IP Routing og KNXnet/IP Tunneling benytter en ukryptert dataoverføring, og er derfor ikke beregnet for bruk på det offentlige internettet. Derfor skal det ikke åpnes noen porter for ruting mot internett. Dette forhindrer at KNX/f@h-kommunikasjonen er synlig på internett.
- Man kan få tilgang til et anlegg fra internett på følgende måte:
    - Tilgang til KNX/f@h-anlegget via VPS-forbindelser: Dette forutsetter en router med VPN-serverfunksjonalitet eller en server.
    - Bruk av produsentspesifikke løsninger eller visning, f.eks. med tilgang via https.

Cyber Security
Disclaimer for Products

Branża jest we wzmożonym stopniu konfrontowana z ryzykiem związanym z bezpieczeństwem internetowym. Aby zwiększyć bezpieczeństwo i odporność swoich rozwiązań, przedsiębiorstwo ABB oficjalnie wprowadziło sprawdzanie odporności w zakresie bezpieczeństwa internetowego w ramach procesu rozwoju produktów.

Następujące wskazówki służą ponadto jako przewodnik i opisują mechanizmy, które można stosować, aby poprawić bezpieczeństwo instalacji KNX / f@h.

Udaremnienie dostępu do różnych mediów

Podstawę każdej koncepcji ochrony stanowi staranne odizolowanie systemu, uniemożliwiające dostęp osobom niepowołanym. W przypadku
KNX / f@h obowiązuje zasada, że fizyczny dostęp do instalacji KNX/f@ mogą mieć wyłącznie osoby uprawnione (instalator, gospodarz domu, użytkownik). Podczas planowania i instalacji należy jak najlepiej chronić krytyczne punkty każdego medium KNX/f@h.
Ogólnie obowiązuje zasada, że aplikacje i urządzenia należy instalować na stałe, aby zapobiec ich łatwemu usunięciu i dzięki temu uzyskaniu dostępu do instalacji KNX/f@h przez osoby niepowołane.
Rozdzielnice z urządzeniami KNX/f@h powinny być zamknięte lub znajdować się w pomieszczeniu, do którego dostęp mają jedynie osoby uprawnione.

Okablowanie twisted pair

- Końcówki skrętek KNX/f@h nie mogą być widoczne i wystawać ze ściany - ani w budynku ani poza nim.
- Jeśli są dostępne, to należy stosować urządzenia zabezpieczające moduły aplikacyjne przed kradzieżą.
- Przewody magistralne na obszarze zewnętrznym stwarzają zwiększone ryzyko. Tu należy szczególnie utrudnić fizyczny dostęp do skrętek KNX/f@h.
- Urządzenia instalowane w obszarze z ograniczoną ochroną (obszar zewnętrzny, garaż podziemny, toaleta itp.) można w celu dodatkowej ochrony wykonać w formie własnej linii. Aktywacja tabeli filtrów w złączu magistralnym (**tylko KNX**) uniemożliwia atakującemu dostęp do całej instalacji.

Okablowanie IP wewnątrz budynku

- Do systemu automatyki budynkowej należy stosować odrębną sieć LAN lub WLAN z własnym oprogramowaniem (routery, przełączniki itp.).
- Niezależnie od mechanizmów bezpieczeństwa przeznaczonych do instalacji KNX/f@h należy bezwzględnie stosować mechanizmy bezpieczeństwa do sieci IP. Są to na przykład:
    - filtry MAC
    - kodowanie sieci bezprzewodowych
    - stosowanie silnych haseł i ich ochrona przed niepowołanymi osobami

Podłączenie do internetu

- Routowanie KNXnet/IP i tunelowanie KNXnet/IP wykorzystują niekodowaną transmisję danych i dlatego nie są przeznaczone do stosowania w internecie publicznym. Z tego względu nie wolno otwierać żadnych portów w kierunku internetu: zapobiega to widoczności komunikacji KNX/f@h w internecie.
- Dostęp do urządzenia przez internet można umożliwić w następujący sposób:
    - Dostęp do instalacji KNX/f@h przez połączenia VPN: wymaga to jednakże routera z funkcją serwera VPN lub serwera.
    - Zastosowanie własnych rozwiązań lub wizulalizacji przez producenta, np. z dostępem przez https.

Cyber Security
Disclaimer for Products

O ramo é confrontado cada vez mais com riscos de segurança na internet. Para aumentar a estabilidade, a segurança e a robustez das suas soluções, dentro do processo de desenvolvimento do produto a ABB introduziu oficialmente os testes de resistência para a segurança na internet.

As seguintes instruções, além disso, servem como guia e descrevem os mecanismos que podem ser usados para melhorar a segurança dos sistemas KNX / f@h.

Impedir o acesso aos diferentes meios

A base de cada conceito de proteção forma o isolamento cuidadoso do sistema contra o acesso não autorizado. No caso de um sistema KNX / f@h, somente as pessoas autorizadas (instalador, porteiro, utilizador) tem um acesso físico ao sistema KNX/f@h. Para o planeamento e a instalação, para cada meio KNX/f@h os pontos críticos devem ser protegidos da melhor forma. Geralmente, as aplicações e os aparelhos devem ser instalados fixos para evitar que estes possam ser facilmente removidos e, com isso, pessoas nao autorizadas tenham acesso ao sistema KNX/f@h.
As subdivisões com os aparelhos KNX/f@h devem ser fechadas ou estar em compartimentos aos quais somente pessoas autorizadas tem acesso.

Cableagem Twisted Pair

- As pontas dos cabos do cabo KNX/f@h Twisted Pair não devem ser visíveis ou sair da parede, nem dentro nem fora do prédio.
- Se disponível, os dispositivos contra o roubo dos módulos de aplicação devem ser usados.
- Os cabos de bus na área externa representam um risco maior. O acesso físico ao cabo KNX/f@h Twisted Pair aqui deve ser especialmente dificultado.
- Os aparelhos, que estão montados nas áreas limitadamente protegidas (área externa, garagem subterrânea, casa de banho, etc.), podem ser executados como proteção adicional como linha própria. Através da ativação das tabelas de filtro no acoplador de linha (**somente KNX**), é impedido que um estranho tenha acesso ao sistema completo.

Cableagem IP dentro do prédio

- Para a automação de edifícios, deve ser usada uma rede separada LAN ou WLAN com hardware próprio (router, interruptores, etc.).
- Independente do sistema KNX/f@h, os mecanismos de segurança comuns para as redes IP devem ser sempre usados. Estes são, por exemplo:
    - Filtro MAC
    - Codificação das redes sem fio
    - Utilização de senhas fortes e proteção desta contra pessoas não autorizadas

Conexão à internet

- KNXnet/IP Routing e KNXnet/IP Tunneling usam uma transmissão de dados não codificada e, por isso, não são previstas para a utilização na internet pública. Por este motivo, nenhum Port do Router podem ser abertos na direação da internet: isto impede que a comunicação KNX/f@h seja visível na internet.
- Um acesso a um sistema a partir da internet pode ser possível da seguinte forma:
    - Acesso às instalações KNX/f@h através de conexões VPN: para isto, porém, é neessário um Router com funcionalidade de servidor VPN ou um servidor.
    - Utilização de soluções específicas do fabricante ou visualizações, p. ex., com acesso através de https.

Cyber Security
Disclaimer for Products

Сегодня отрасль все чаще сталкивается с проблемами, связанными с безопасностью в Интернете. Для того чтобы повысить безопасность и надежность своих решений, компания ABB официально внедрила в практику разработки своей продукции испытания на безопасность работы в Интернете.

Следующие указания в дополнение к вышесказанному описывают механизмы, позволяющие повысить безопасность систем на базе KNX / f@h.

Предотвращение доступа к различным информационным средствам

Основой любой концепции безопасности является тщательная защита системы от несанкционированного доступа. В случае с системой KNX / f@h физический доступ к ней должны иметь только уполномоченные лица (установщики, техники-смотрители, пользователи).

При проектировании и установке должны быть наилучшим образом защищены критические точки каждого средства KNX/f@h.

Приложения и устройства должны устанавливаться стационарно и с обеспечением надежной защиты от несанкционированного доступа посторонних лиц к системе KNX/f@h.

Вторичные распределительные пункты с устройствами KNX/f@h должны запираться или находиться в помещениях, доступ в которые возможен только для уполномоченных лиц.

Проводка с использованием двухпроводного крученого кабеля

- Концы проводов витых пар KNX/f@h должны быть скрытыми и не выступать за поверхность стен, как внутри, так и снаружи здания.
- При наличии такой возможности следует использовать устройства защиты от кражи модулей приложений.
- Прокладка шинных линий связи под открытым небом влечет за собой повышенные риски. В этом случае следует обеспечить усиленную защиту от физического доступа к витой паре KNX/f@h.
- Устройства, которые монтируются в зонах с ограниченной защитой (под открытым небом, в подземных гаражах, туалетах и т. д.), для повышения уровня защиты могут быть выполнены в виде отдельной линии. С помощью активации таблиц фильтров в линейном коплере (**только KNX**) можно предотвратить доступ посторонних лиц к общей системе.

IP-проводка внутри здания

- В системе автоматизации здания следует использовать автономную сеть LAN или WLAN с собственной аппаратной частью (маршрутизаторы, коммутаторы и т. д.).
- Независимо от системы KNX/f@h необходимо обязательно использовать традиционные механизмы обеспечения безопасности IP-сетей. К таковым, например, относятся:
    - MAC-фильтры
    - Шифрование беспроводных сетей
    - Использование надежных паролей и их защита от несанкционированного доступа

Подключение к Интернету

- В KNXnet/IP-маршрутизации и KNXnet/IP-туннелировании используется передача данных без шифрования, в связи с чем эти режимы не предназначены для использования в общедоступной сети Интернет В связи с этим запрещается открывать порты маршрутизаторов в направлении Интернета, в противном случае будет возможность отслеживания обмена данными по KNX/f@h через Интернет.
- Доступ к системе через Интернет может быть обеспечен следующим образом:
    - Доступ к KNX/f@h через VPN-соединения: такой способ, однако, предполагает наличие маршрутизатора с поддержкой функционала VPN-сервера и самого сервера.
    - Использование индивидуальных решений и систем визуализации, например, доступ по https.

Cyber Security
Disclaimer for Products

Branschen konfronteras allt mer med risker avseende internetsäkerhet. För att öka stabiliteten, säkerheten och robustheten på sina lösningar har ABB officiellt infört robusthetstester för internetsäkerhet inom ramen för produktutvecklingsprocessen.

Därutöver fungerar följande anvisningar som guider och beskriver mekanismer som kan användas för att förbättra säkerheten hos KNX-/f@h-anläggningar.

Förhindra åtkomst till de olika medierna

Grunden i alla skyddskoncept är att systemet noggrant skyddas mot obehörig åtkomst. Vid KNX-/f@h-anläggningar gäller att endast behöriga personer (installatör, vaktmästare, användare) får ha fysisk åtkomst till dem.
Vid planering och installation måste de kritiska punkterna i varje KNX-/f@h-medium skyddas så bra som möjligt.
Generellt gäller att användningsställen och enheter ska monteras fast för att förhindra att de enkelt tas bort och därigenom ger obehöriga personer åtkomst till KNX-/f@h-anläggningen.
Undergruppcentraler med KNX-/f@h-enheter ska vara stängda eller monterade i ett rum till vilka endast behöriga personer har tillträde.

Twisted Pair-ledningsinstallation

- Ledningsändarna i KNX-/f@h-Twisted Pair-kablarna får inte vara synliga eller sticka ut ur väggen, varken inne i eller utanför byggnaden.
- Om de är tillgängliga ska applikationsmodulens stöldskydd användas.
- Bussledningar utomhus innebär en förhöjd risk. Fysisk åtkomst till KNX-/f@h-Twisted Pair-kabeln ska försvåras.
- Enheter som är monterade i begränsat skyddade områden (utomhus, underjordsgarage, WC etc.) kan göras som egen linje som ytterligare skydd. Genom att aktivera filtertabellerna i linjekopplaren (**endast KNX**) förhindras att angripare får åtkomst till hela anläggningen.

IP-ledningsinstallation i byggnaden

- I byggnadsautomationen bör ett separerat LAN- eller WLAN-nätverk med egen hårdvara (router, switches etc.) användas.
- Oberoende av KNX-/f@h-anläggningen ska de vedertagna säkerhetsmekanismerna för IP-nätverk användas. Det är exempelvis:
    - MAC-filter
    - Kryptering av trådlösa nätverk
    - Använda säkra lösenord och skydda dem från obehöriga personer

Anslutning till internet

- Vid KNXnet/IP-routing och Xnet/IP-tunnling används en okrypterad dataöverföring och är därför inte avsedda för att användas på internet. Därför får inga av routerns portar i riktning mot Internet öppnas; det förhindrar att KNX-/f@h-kommunikationen syns på Internet.
- ör att få åtkomst till ett system på internet kan man gå till väga på följande sätt:
    - Åtkomst till KNX-/f@h-installationen via VPN-förbindelser: det förutsätter dock en router med VPN-serverfunktion eller en server.
    - Använda tillverkarspecifika lösningar eller visualieringar, t.ex. med åtkomst via https.

Cyber Security
Disclaimer for Products

行业目前正遭受网络安全风险的严重威胁。为了提高行业解决方案的稳定性、安全性和鲁棒性，ABB 在产品研发过程中正式引入了鲁棒性检测流程，以确保网络完全。

此外，以下提示用作操作手册，并说明可能使用的机制，以提高 KNX / f@h 设备的安全性。

避免接触各种媒介

每种保护方案的基础都是小心隔离系统，以防擅自访问。针对
对于 KNX / f@h 设备，只有授权任运（装配人员、管理人、用户）才能物理访问 KNX/f@h 设备。在规划和安装时，必须针对每种 KNX/f@h 媒介尽量保护重要点。
通常，在应用程序和设备安装时，应避免被轻易够到，从而导致未授权人员也能接触 KNX/f@h 设备。
带 KNX/f@h 设备的配电箱应关闭，或位于仅有授权人员才能访问的室内。

双绞线布线

- KNX/f@h 双绞线电缆的线端不应被看见或从墙壁中凸出，既不得在建筑内，也不得在建筑外。
- 如果可用，应使用防盗保护设施或应用模块。
- 在外部区域的总线导线风险会提高。在此应特别限制对 KNX/f@h 双绞线电缆的物理接触。
- 安装在有限保护区域的设备（外部区域、卫生间等），可以作为独立线路额外保护。通过激活线路耦合器（**仅限 KNX**）中的过滤板，可以避免干扰物进入整个设备。

建筑内的 IP 布线

- 对于楼宇自动化系统，应使用带有各自硬件（路由器、交换机等）的独立 LAN 或 WLAN 网络。
- 无论哪种 KNX/f@h 设备，务必使用适用于 IP 网络的普通安全机制。比如：
    - MAC 过滤器
    - 无线网络加密
    - 使用复杂的密码并防止未授权人员使用

连接互联网

- KNXnet/IP Routing 和 KNXnet/IP Tunneling 为非加密式数据传输方式，因此请勿设计用于公共因特网网络中。因此，禁止打开因特网网络方向的路由器端口，这可避免因特网网络内的 KNX/f@h 通信被看见。
- 可以通过下列方式从互联网访问设备：
    - 通过 VPN 连接访问 KNX/f@h 装置：但前提是使用了具有 VPN 服务器功能的路由器或服务器。
    - 使用制造商特定的解决方案或可视化系统，例如通过 https 访问。

Cyber Security
Disclaimer for Products

Branže je stále silněji konfrontována s bezpečnostními riziky internetu. Aby zvýšila stabilitu, bezpečnost a robustnost svých řešení, zavedla společnost ABB v rámci procesu vývoje produktů oficiálně zkoušky robustnosti pro zabezpečení sítě Internet.

Následující upozornění slouží také jako vodítko a popisují mechanismy, které lze aplikovat, aby se zlepšila bezpečnost zařízení KNX / f@h.

Zamezení přístupu k různým médiím

Základem každého konceptu ochrany je pečlivé zabezpečení systému před neoprávněným přístupem. V případě systému KNX / f@h platí, že jen povolané osoby (instalatér, domovník, uživatel) smí mít fyzický přístup k systému KNX/f@h. Při plánování a instalaci musí být co nejlépe chráněny kritické body pro každé médium KNX/f@h.
Obecně platí, že aplikace a přístroje by měly být pevně instalovány, aby se zabránilo, že by mohly být snadno odebrány a tím by nepovolané osoby získaly přístup k zařízení KNX/f@h.
Podružné rozvody k přístrojům KNX/f@h by měly být uzavřené nebo se nacházet v místnostech, do kterých mají přístup jen povolané osoby.

Kabeláž Twisted Pair

- Koncovky vedení kabelu KNX/f@h Twisted Pair nesmí být viditelné nebo vyvedeny ze stěny, ani v budově, ani mimo budovu.
- Jestliže jsou dostupné, je třeba použít zařízení na ochranu před krádeží aplikačních modulů.
- Sběrnicová vedení vedená venku představují zvýšené riziko. Fyzický přístup ke kabelu KNX/f@h Twisted Pair by zde měl být obzvláště ztížen.
- Přístroje, které jsou instalovány v omezeně chráněných prostorách (venku, v podzemní garáži, na WC, apod.), lze pro dodatečnou ochranu realizovat jako samostatnou linku. Aktivací tabulek filtrů ve vazebném členu linky (pouze KNX) se zabrání, aby útočník mohl získat přístup k celému systému.

IP kabeláž uvnitř budovy

- Pro automatizaci budovy je nutno použít oddělenou síť LAN nebo WLAN s vlastním hardwarem (router, přepínače atd.).
- Nezávisle na systému KNX/f@h se bezpodmínečně musí použít bezpečnostní mechanismy obvyklé pro IP sítě. Na příklad to je:
    - MAC filtr
    - Zakódování bezdrátových sítí
    - Použití silných hesel a jejich ochrana před nepovolanými osobami

Připojení k Internetu

- KNXnet/IP Routing a KNXnet/IP Tunneling využívají nekódovaný datový přenos a nejsou proto určeny k použití na veřejném Internetu. Z tohoto důvodu se nesmí otevřít žádné porty routerů směrem na Internet: tím se zabrání, aby komunikace KNX/f@h byla na Internetu viditelná.
- Přístup k systému z Internetu lze umožnit následujícím způsobem:
    - Přístup k instalacím KNX/f@h přes připojení VPN: podmínkou je však router s funkcí VPN serveru nebo server.
    - Použití řešení specifických pro daného výrobce nebo vizualizací, např. s přístupem přes https.

Cyber Security
Disclaimer for Products

Sektörümüzde, internet güvenliği alanında çok yüksek riskler söz konusudur. ABB, çözümlerin güvenlik, sağlamlık ve dayanıklılık özelliklerini daha da geliştirmek için, ürün geliştirme süreci çerçevesinde internet güvenliğine yönelik resmi sağlamlık testlerini hayata geçirmiştir.

Aşağıdaki bilgiler ayrıca bir kılavuz niteliğindedir ve KNX / f@h sistemlerinin güvenlik özelliklerini iyileştirmek için kullanılabilecek mekanizmaları açıklar.

Farklı ortamlara erişimi engelleme

Her türlü koruma konseptinin temelinde, yetkisiz erişimleri engellemek amacıyla sistemlerde uygun bölümlendirmelerin dikkatlice gerçekleştirilmesi yatar. Bir KNX / f@h sistemi söz konusu olduğunda, sadece yetkili kişilerin (tesisatçı, temizlikçi, kullanıcı) KNX/f@h sistemine fiziksel erişime sahip olması gerekir. Planlama ve kurulum sırasında, tüm KNX/f@h ortamları için kritik önemdeki noktalar mümkün olan en iyi şekilde korumaya alınmalıdır.
Genel olarak uygulamalar ve cihazlar sabit şekilde kurulmalıdır, aksi halde bunlar kolayca çıkartılabilir ve yetkisiz kişiler tarafından KNX/f@h sistemine erişim sağlanabilir.
KNX/f@h cihazlar ile yapılan alt dağıtımlar kapalı olmalı veya sadece yetkili kişilerin erişebileceği alanlarda bulunmalıdır.

Twisted Pair (Çift Bükümlü) kablo sistemi

- KNX/f@h Twisted Pair kablonun uçları görünmemeli veya binanın içinde ya da dışında duvarlardan dışarı çıkmamalıdır.
- Mevcutsa, uygulama modüllerindeki hırsızlık önleme tertibatları kullanılmalıdır.
- Dış alandaki bus hatları büyük bir risk oluşturur. KNX/f@h Twisted Pair kabloya fiziksel erişim burada özellikle çok daha zor olmalıdır.
- Sınırlı korumaya sahip alanlara (dış mekan, alçak garaj, tuvalet, vs.), monte edilen cihazlarda, ilave bir koruma önlemi olarak her bir cihaz ayrı hatta bağlanabilir. Hat birleştiricideki filtre tablolarının etkinleştirilmesi ile (sadece KNX), bir saldırganın tüm sisteme erişime sahip olması önlenir.

Bina içindeki IP kablo sistemi

- Bina otomasyonu için, kendi donanımına (yönlendirici, anahtarlar vs.) sahip ayrı bir LAN veya WLAN ağı kullanılmalıdır.
- KNX/f@h sisteminden bağımsız olarak, IP ağlarına yönelik klasik güvenlik mekanizmaları kullanılmalıdır. Bunlar örneğin:
    - MAC filtresi
    - Kablosuz ağları şifreleme
    - Daha güçlü şifreler kullanma ve bunları yetkisiz kişilerden koruma

İnternete bağlanma

- KNXnet/IP Routing ve KNXnet/IP Tunneling, şifresiz bir veri aktarımı gerçekleştirir ve dolayısıyla kamuya açık internet bağlantısı ile kullanımı öngörülmemiştir. Bu nedenle, yönlendiricilerden internete doğru kapı (port) açılmamalıdır: bu sayede KNX/f@h iletişiminin internet üzerinde görünür hale gelmesi önlenir.
- İnternetten sisteme erişim aşağıdaki şekilde gerçekleştirilebilir:
    - KNX/f@h kurulumlarına VPN bağlantıları üzerinden erişim: Bu seçenek için VPN sunucusu işlevine sahip bir yönlendiricinin veya bir sunucunun mevcut olması şarttır.
    - Üreticiye özel çözümler veya görselleştirmeler kullanma, örn. https üzerinde erişim.