Guide de cybersécurité

hw+

Disjoncteurs sentinel Energy

HW1, HW2 et HW4

hager

Sommaire

Page

Avertissements et remarques

Cette documentation contient des consignes de sécurité, que vous devez respecter pour votre sécurité personnelle ou pour la prévention des dommages aux biens.
Les consignes de sécurité, se référant à votre sécurité personnelle sont notifiées dans la documentation par un symbole d'alerte de sécurité. Les consignes de sécurité, se référant à des dommages matériels sont informées par la mention "AVIS".
Les symboles d'alerte de sécurité et de la mention ci-dessous sont classés selon le degré de risque.

DANGER

DANGER indique une situation dangereuse imminente qui, si elle ne peut pas être évitée, entraînera la mort ou des blessures graves.

AVERTISSEMENT

AVERTISSEMENT indique une situation potentiellement dangereuse qui, si elle ne peut pas être évitée, peut entraîner des blessures grave voire la mort.

ATTENTION

ATTENTION indique une situation potentiellement dangereuse qui, si elle ne peut pas être évitée, peut provoquer des blessures mineures ou modérées.

AVIS

AVIS indique un message d'alerte de dommages matériels.
AVIS indique également des consignes importantes d'utilisation et surtout des informations utiles sur le produit, auxquelles il convient de prêter une attention particulière pour une utilisation efficace et en toute sécurité.

Personnel qualifié

Le produit ou le système décrit dans cette documentation doit être installé, exploité et maintenu par un personnel qualifié uniquement. Hager Electro décline toute responsabilité quant aux conséquences de l'utilisation de ce matériel par un personnel non qualifié.
Une personne qualifiée est celle disposant de compétences et des connaissances nécessaires à la construction et l'exploitation de l'installation des équipements électriques, et ayant reçu une formation lui permettant d'identifier et d'éviter les risques encourus.

Usage approprié des produits Hager

Les produits Hager sont destinés à être utilisés uniquement pour les applications décrites dans les catalogues et sur la documentation technique, qui leur est dédiée. Si des produits et des composants provenant d'autres fabricants sont utilisés, ils doivent être recommandés ou approuvés par Hager.
Un usage approprié des produits Hager lors du transport, du stockage, de l'installation, du montage, de la mise en service, de l'exploitation et de l'entretien est nécessaire pour garantir un fonctionnement en toute sécurité et sans aucun problème.
Les conditions ambiantes admissibles doivent être respectées. Les informations contenues dans la documentation technique doivent être respectées.

Responsabilité de publication

Les contenus de cette documentation ont été revus afin d'assurer que la fiabilité de l'information soit correcte au moment de la publication.
Hager ne peut toutefois pas garantir l'exactitude de toutes les informations contenues dans cette documentation. Hager n'assume aucune responsabilité pour les erreurs d'impression et des dommages qui en résultent.
Hager se réserve le droit d'apporter les corrections et modifications nécessaires dans les éditions ultérieures.

Cybersécurité et connexion sans fil

Le produit ou le système décrit dans cette documentation nécessite la mise en place de mesures de protection contre les risques inhérents à toute connexion et transmission sans-fil et les risques inhérents à toute connexion et transmission filaire.

AVERTISSEMENT

Risques de piratage à distance par connexion sans-fil
- Maintenez la connexion Bluetooth Low Energy désactivée, si vous n'utilisez pas l'application Hager Power touch.
- Evitez d'activer la connexion Bluetooth Low Energy, si vous n'êtes pas en mesure d'interdire tout accès non autorisé aux appareils installés.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

AVERTISSEMENT

Risques pouvant affecter la disponibilité, l'intégrité et la confidentialité du système sentinel Energy
- Modifiez les mots de passe par défaut à la première utilisation, afin d'empêcher tout accès non autorisé aux réglages, contrôles et informations des appareils.
- Désactivez les ports et services inutilisés, ainsi que les comptes par défaut, pour réduire le risque d'attaques malveillantes.
- Protégez les appareils en réseau par plusieurs niveaux de cyberdéfense (pare-feu, segmentation du réseau, détection des intrusions et protection du réseau).
- Respectez les bonnes pratiques de cybersécurité (par exemple : moindre privilège, séparation des tâches) pour réduire les risques d'intrusion, la perte ou l'altération des données et journaux, ou l'interruption des services.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Objet du document

Ce document est conçu pour fournir aux installateurs électriques, aux intégrateurs systèmes ou aux concepteurs de systèmes les éléments de cybersécurité des disjoncteurs hw+ équipés de déclencheurs électroniques sentinel Energy. Cela afin d'aider les concepteurs et les utilisateurs de ces systèmes à mettre en œuvre un environnement sécurisé d'exploitation du produit.

Champ d'application

Le présent document s'applique aux disjoncteurs hw+ équipés de déclencheurs électroniques sentinel Energy.

Révisions

Indice	Date
6LE009347A	Décembre 2023

Documents à consulter

Document	Référence
Manuel d'installation HW1	6LE007596A
Manuel d'installation HW2 et HW4	6LE009207A
Manuel d'utilisation Déclencheurs électroniques sentinel Energy hw+	6LE008146A
Guide utilisateur Communication Modbus sentinel Energy	6LE007962A

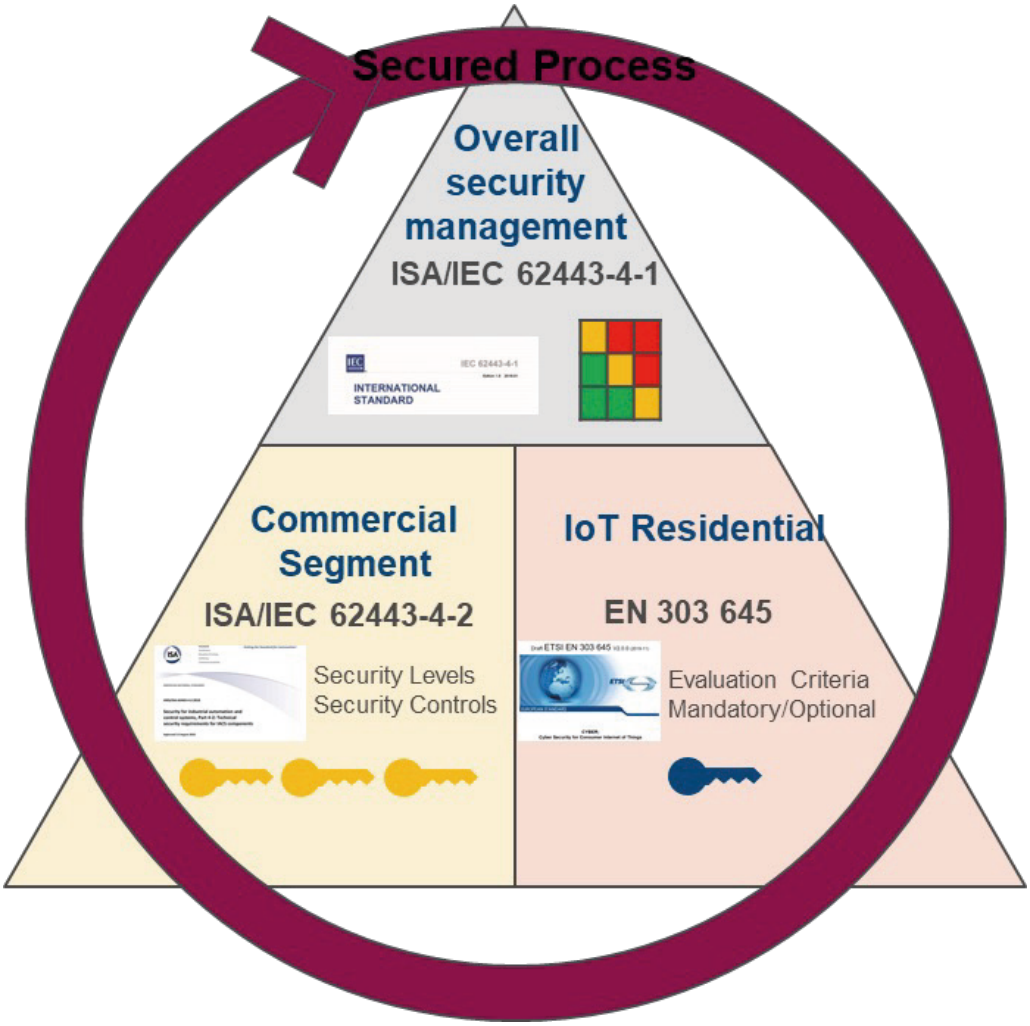
Vous pouvez télécharger ces publications et autres informations techniques depuis notre site web à l'adresse : www.hager.com

Contact

Adresse	Hager Electro SAS 132 Boulevard d'Europe 67215 Obernai France
Téléphone	+ 33 (0)3 88 49 50 50
Site internet	www.hager.com

Hager porte une attention particulière aux questions de protection des données et de sécurité de connexion de ses produits connectés.
C'est pourquoi nous mettons en œuvre toutes les dispositions pour atteindre les meilleurs standards de qualité en terme de sécurité des données véhiculées par nos produits.

Hager utilise les normes CEI 62443 et EN 303 645 dans la conception et développement de ses produits connectés.
La suite de norme CEI 62443 s'applique au fonctionnement sécurisé des systèmes d'automatisation industriels (systèmes ICS) de la conception jusqu'à la gestion, en passant par l'implantation.
La norme EN 303 645 définit des dispositions de haut niveau en matière de cybersécurité et de protection des données pour les appareils IoT grand public connectés.



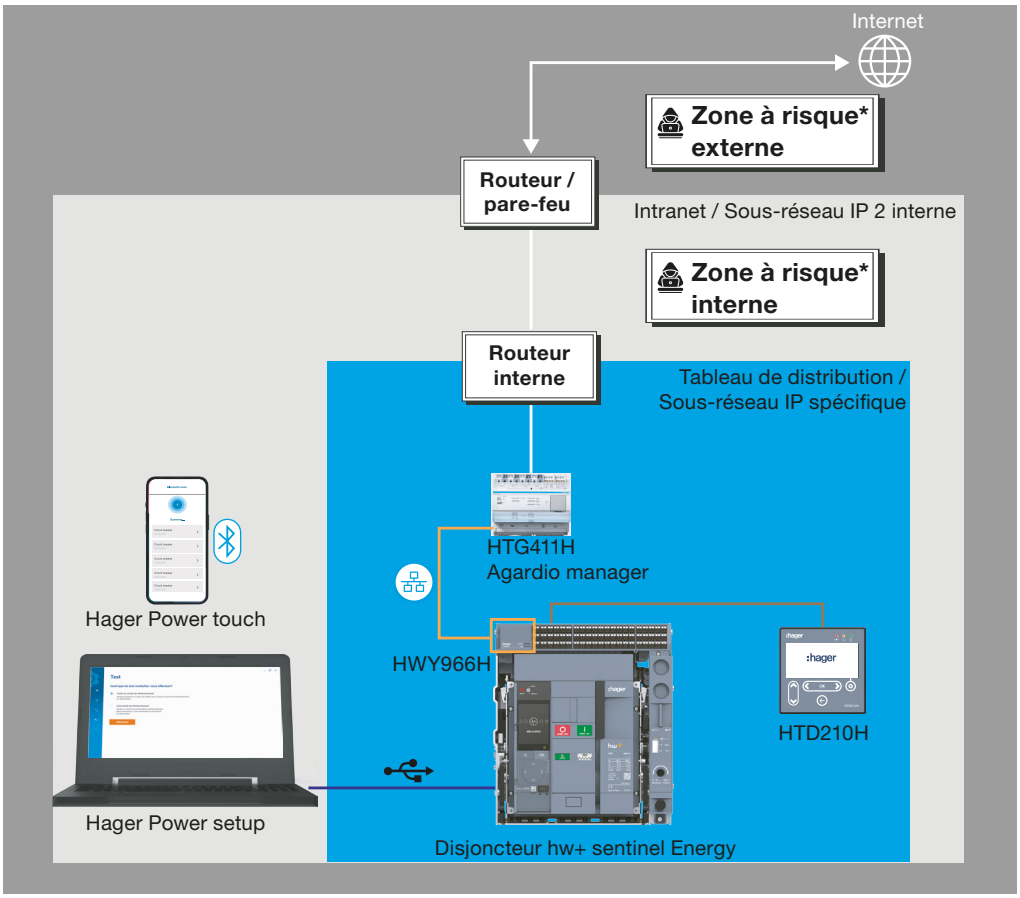
L'application d'un processus sécurisé pendant les phases de conception, de développement et de validation, empêche également les attaques visant à perturber vos produits ou à modifier la configuration de votre système.

2.2.1 Environnement du système sentinel Energy

Le disjoncteur hw+ sentinel Energy est un élément crucial d'une distribution électrique ou un équipement électrique car il assure la protection électrique.

Grâce à ses fonctions de communication, il assure l'accès à des fonctions de contrôle en temps réel et à des données de surveillance de la distribution électrique. Cela permet une plus grande efficacité et flexibilité dans la gestion de votre installation électrique. Cependant, ces fonctions vous exposent à des cyberattaques potentielles.

La figure suivante illustre l'environnement de communication dans lequel s'intègre le disjoncteur hw+ sentinel Energy.



Légende :

	Internet
	Intranet
	Tableau de distribution
	Communication modbus
	USB-C
	Port CIP pour protocole propriétaire
	Bluetooth Low Energy

(*) Risque d'attaques ou de compromissions

Le système sentinel Energy permet de communiquer avec le disjoncteur hw+ par l'un des moyens suivants :
- l'interface afficheur/clavier du déclencheur sentinel Energy,
- la connexion Bluetooth Low Energy (BLE) sans fil depuis un smartphone embarquant l'application Hager Power touch,
- la connexion par port USB-C au logiciel Hager Power setup,
- la connexion par liaison série à protocole propriétaire CIP à l'afficheur déporté HTD210H,
- la connexion à un réseau de liaison série RS 485 à l'aide du protocole Modbus-RTU,
- la connexion à un réseau Ethernet à l'aide du protocole Modbus-TCP.

Chacun de ces moyens de communication représente une vulnérabilité dans votre système, si les mesures de sécurité appropriées ne sont pas mises en place.
Notamment votre système s'expose aux risques suivants si les mesures de sécurité appropriées ne sont pas mis en place :
- risque d'indisponibilité du système conduisant à un black-out,
- risque de modification des paramètres du système par des personnes non-autorisées conduisant à des dysfonctionnements et à l'absence de protection électrique,
- risque de prise de contrôle du système par des personnes non-autorisées conduisant à une cyber-attaque,
- risque de perte de données essentielles et sensibles par cyber-attaque et de chantage à la rançon.

Ce guide fournit nos recommandations pour sécuriser ces moyens de communication et éviter les attaques intentionnelles ou une mauvaise utilisation accidentelle.

2.2.2 Fonctionnalités de sécurité

Les fonctionnalités de sécurité suivantes ont été intégrées lors de la conception afin d'atténuer les menaces inhérentes au déploiement du système sentinel Energy dans un environnement connecté :

- sécurisation de la communication Bluetooth à l'aide de l'algorithme AES,
- actions de modification des réglages et actions de contrôle/commande accessibles qu'après la saisie de mots de passe ou de codes personnalisés,
- communication IP chiffrée,
- activation du chiffrement et de l'authentification de la communication Modbus,
- gradation du niveau de sécurité lors des commandes d'écriture dans les registres Modbus.

Ces fonctionnalités de sécurité ainsi que le fonctionnement du système sentinel Energy ont été vérifiés par des organismes tierce-partie externes et indépendants lors de l'exécution de tests de pénétration (simulation d'attaques d'un utilisateur mal intentionné ou d'un logiciel malveillant).

La technologie opérationnelle (OT) désigne le matériel et les logiciels utilisés pour surveiller les dispositifs et les processus physiques au sein d'une entreprise. Lors de son déploiement il est important d'identifier et de protéger les informations essentielles ou sensibles aux opérations d'une entreprise.

Voici une liste non exhaustive d'informations sensibles :
- les codes d'accès des équipements ou des locaux sous clé,
- l'architecture système,
- les adresses IP ou MAC des équipements de communication connectés,
- les numéros de port utilisés pour la communication Ethernet,
- les identifiants et mots de passe des utilisateurs.

A cela s'ajoutent les informations fournies par le système sentinel Energy.

	Afficheur sentinel Energy	**Afficheur déporté HTD210H**	**Bluetooth**	**USB-C**	**Modbus-RTU Modbus-TCP**
Modbus-TCP					
Surveillance des données	Lecture	Lecture	Lecture	Lecture	Lecture
Paramètre de protection du disjoncteur	Lecture/ Ecriture	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Autres paramètres du disjoncteur	Lecture/ Ecriture	Lecture/ Ecriture	Lecture	Lecture/ Ecriture	Lecture/ Ecriture
Commandes d'ouverture et de fermeture	Oui	Non	Oui	Oui	Oui
Réinitialisations	Oui	Oui	Non	Oui	Oui

L'un des points clés d'une stratégie de défense contre les cyberattaques est d'appliquer une politique efficace de mot de passe.

AVERTISSEMENT

Risques pouvant affecter la disponibilité, l'intégrité et la confidentialité du système sentinel Energy
Modifiez les mots de passe par défaut à la première utilisation, afin d'empêcher tout accès non autorisé aux réglages, contrôles et informations des appareils.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Cela passe par les meilleures pratiques suivantes (liste non exhaustive) :
- Modifier tous les mots de passe par défaut.
- Définir des mots de passe forts: les choix triviaux tels que "1234" ou "mot de passe" doivent être évités.
- Ne pas partager ses mots de passe avec des personnes non autorisées ou non habilitées.
- Changer ses mots de passe régulièrement.
- Ne pas réutiliser les anciens mots de passe.
- Stocker les mots de passe dans un lieu sûr (par exemple un coffre à mots de passe).

Cette politique de mot de passe doit être appliquée à tous les composants du système sentinel Energy, aux serveurs, ordinateurs, aux smartphones connectés au système et à tout autre composant réseau.

La cybersécurité concerne tous les employés de l'entreprise. Notamment tous les utilisateurs autorisés à accéder au système sentinel Energy et au réseau de communication de l'installation, doivent connaitre la stratégie de protection des informations de l'entreprise.

Ils doivent de plus avoir suivi une formation aux principes fondamentaux de la cybersécurité et aux règles d'exécution découlant de cette stratégie.

De façon régulière, il est nécessaire de rappeler les bonnes pratiques suivantes (et sans s'y limiter) :

- suivre la stratégie de mot de passe,
- ne pas partager les mots de passe, les codes d'accès et les données sensibles,
- s'assurer que tous les ordinateurs connectés au système (mise en service, surveillance, contrôle...) sont à jour et sont protégés contre les virus et les logiciels malveillants,
- si les ordinateurs sont également utilisés pour l'envoi de messages, les utilisateurs doivent être formés pour détecter les courriers suspects,
- tous les smartphones utilisés pour accéder au système doivent être protégés par un code PIN ou une reconnaissance faciale et doivent être protégés contre le piratage sur Internet et par Bluetooth,
- tous les smartphones doivent conserver leur intégrité système ainsi que de ses composants,
- tous les smartphones utilisés pour accéder au système doivent toujours rester en possession des utilisateurs et ne pas être partagé,
- les politiques de sécurité en place ne doivent pas être contournées.

L'accès à proximité du déclencheur sentinel Energy embarqué dans le disjoncteur hw+ permet d'accéder à toutes ses fonctionnalités, notamment ses paramètres de protection et de contrôle à distance.

Il est par conséquent important de restreindre son accès en installant le disjoncteur dans un local sous clé ou protégé par code d'accès pour éviter :
- tout accès non autorisé à l'afficheur sentinel Energy et son clavier, évitant tout risque de modification de paramètres de réglage et de contrôle,
- tout accès non autorisé à la communication Bluetooth sans fil, évitant le risque de prise de contrôle avec l'application Hager Power touch,
- toute connexion non autorisée via le port USB-C pour éviter tout risque de modification de paramètres depuis le logiciel Hager Power setup.

En particulier, vous devez vérifier que :
- le local est maintenu sous clé à tout moment,
- le local est équipé d'un système d'authentification et d'autorisation,
- seul le personnel autorisé dispose d'une clé ou du code d'accès,
- les câbles du réseau de communication qui entrent dans le local et les ports de connexion sur les équipements de communication hors de la salle sont protégés,
- tous les équipements (ordinateur, smartphones et tablettes) qui ont accès au déclencheur sentinel Energy bénéficient d'une protection renforcée conformément aux dernières consignes en date du fournisseur.

Toute personne ayant l'accès au tableau de distribution, dans lequel est installé le disjoncteur hw+, peut accéder à l'afficheur sentinel Energy, à son clavier et modifier ainsi les paramètres de réglage du disjoncteur.

Voici nos recommandations pour se prémunir de tout acte malveillant ou involontaire par accès à l'afficheur sentinel Energy et son clavier :
- activer la protection par mot de passe pour la modification de tous les paramètres (hormis ceux de réglage de l'écran d'affichage),
- activer le verrouillage du clavier sentinel Energy,
- sceller la fenêtre transparente de protection du déclencheur,
- communiquer le mot de passe du déclencheur sentinel Energy uniquement aux personnes autorisées,
- éviter de consigner ce mot de passe sur le smartphone où est installée l'application Hager Power touch (sms, email, notes…).

La connexion par communication Bluetooth permet à un smartphone exécutant l'application Hager Power touch d'accéder en lecture aux informations du déclencheur sentinel Energy et d'engager une commande d'ouverture ou de fermeture du disjoncteur hw+.

Voici nos recommandations pour se prémunir de tout acte malveillant ou involontaire par accès à la connexion Bluetooth :
- installer le disjoncteur hw+ dans un local maintenu sous clé ou dont l'accès est protégé à tout moment,
- seules les personnes autorisées ont accès au local,
- le mot de passe du déclencheur sentinel Energy ne doit être communiqué qu'aux personnes autorisées.

Utilisation de l'application Hager Power touch
L'application Hager Power touch permet de surveiller les informations fournies par le déclencheur sentinel Energy, notamment l'état de fonctionnement du disjoncteur et les valeurs des grandeurs mesurées.
Elle permet également d'effectuer une commande d'ouverture ou de fermeture du disjoncteur hw+, si les accessoires adéquats ont été installés sur le disjoncteur.

A la première connexion le jumelage du smartphone exécutant l'application Hager Power touch avec le disjoncteur, nécessite une action physique sur le déclencheur sentinel Energy. A partir de la deuxième connexion, le jumelage n'est plus requis. La connexion sera établie automatiquement avec le smartphone, si la communication Bluetooth est activée et si l'appareil se trouve à portée de l'émission Bluetooth Low Energy.
Pour plus d'information sur cette application se reporter au Manuel d'utilisation déclencheurs électroniques sentinel Energy hw+.

Il est par conséquent indispensable d'éviter tout risque de piratage par la communication Bluetooth avec l'application Hager Power touch.

⚠ AVERTISSEMENT

Risques de piratage à distance par connexion sans-fil
- Maintenez la connexion Bluetooth Low Energy du déclencheur désactivée, si l'application Hager Power touch n'est pas agrée par votre service informatique.
- Désactivez la connexion Bluetooth Low Energy du déclencheur en cas de non utilisation prolongée de l'application Hager Power touch.
- Supprimez le disjoncteur hw+ de vos appareils Bluetooth connus par votre smartphone en cas de non utilisation prolongée de l'application Hager Power touch.
- Evitez d'activer la connexion Bluetooth Low Energy du déclencheur si vous n'êtes pas en mesure d'interdire tout accès non autorisé aux appareils installés.

Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

La connexion au port USB-C à l'aide du logiciel Hager Power setup permet d'accéder aux fonctions de protection et aux fonctions de contrôle du déclencheur sentinel Energy.

⚠ AVERTISSEMENT

Risques pouvant affecter la disponibilité, l'intégrité et le fonctionnement du disjoncteur hw+
Scellez la fenêtre transparente de protection du déclencheur, si vous n'êtes pas en mesure d'interdire tout accès non autorisé au disjoncteur.
Le non-respect de ces instructions peut provoquer la mort, des blessures graves ou des dommages matériels.

Pour se connecter au port USB-C il est nécessaire de remplir les conditions suivantes :
- avoir physiquement accès à la prise USB-C située sur le déclencheur sentinel Energy,
- avoir installé le logiciel Hager Power setup sur un ordinateur portable,
- raccorder cet ordinateur au déclencheur à l'aide d'un adaptateur USB-C.

Voici nos recommandations pour l'utilisation du logiciel Hager Power setup :

Il existe de nombreuses attaques qui exploitent les failles du système d'exploitation Microsoft Windows. C'est pourquoi l'ordinateur sur lequel est installé Hager Power setup doit être sécurisé :
- l'ordinateur doit être doté d'un antivirus installé, actif et à jour,
- l'ordinateur doit être configuré pour fonctionner par session (Identifiant + mot de passe),
- les politiques de mots de passe et d'utilisations de l'ordinateur doivent être respectées,
- le logiciel Hager Power setup doit bénéficier des dernières mises à jour.

L'afficheur déporté HTD210H permet d'accéder à plusieurs fonctionnalités du déclencheur, notamment ses paramètres de protection.

Il est par conséquent important de restreindre son accès en installant le disjoncteur dans un local sous clé ou protégé par code d'accès pour éviter :
- tout accès non autorisé à l'afficheur sentinel Energy et son clavier, évitant tout risque de modification de paramètres de réglage et de contrôle,
- tout accès non autorisé à la communication Bluetooth sans fil, évitant le risque de prise de contrôle avec l'application Hager Power touch,
- toute connexion non autorisée via le port USB-C pour éviter tout risque de modification de paramètres depuis le logiciel Hager Power setup.

En particulier, vous devez vérifier que :
- le local est maintenu sous clé à tout moment,
- le local est équipé d'un système d'authentification et d'autorisation,
- seul le personnel autorisé dispose d'une clé ou du code d'accès.

Voici nos recommandations pour se prémunir de tout acte malveillant ou involontaire par accès à l'afficheur déporté HTD210H :
- modifier le mot de passe de l'afficheur HTD210H à la première utilisation,
- activer le verrouillage du clavier de l'afficheur,
- sceller la fenêtre transparente de protection du déclencheur,
- communiquer le mot de passe de l'afficheur uniquement aux personnes autorisées.

Le disjoncteur hw+ équipé d'un déclencheur sentinel Energy offre deux possibilités d'accès distant :
- via un réseau de liaison série RS 485 à l'aide du protocole Modbus RTU dans le cas du module de communication HWY965H,
- via un réseau Ethernet à l'aide du protocole Modbus TCP/IP dans le cas du module de communication HWY966H.

Cet accès distant permet d'accéder à toutes les fonctionnalités du déclencheur sentinel Energy, notamment les paramètres de protection et de contrôle à distance.

Il est par conséquent important de d'activer le verrouillage de l'accès distant, si l'accès en écriture aux paramètres du déclencheur et l'accès aux fonctions de contrôle à distante ne sont pas requises à distance.

Le verrouillage de l'accès distant s'effectue depuis le déclencheur sentinel Energy.
Se reporter au Manuel d'utilisation Déclencheurs électroniques sentinel Energy hw+ pour d'information.

Afin de sécuriser l'accès disant, nous préconisons les recommandations suivantes :
- ne pas faire de redirection de ports au niveau du modem routeur. Cela exposerait votre interface Modbus ou votre configurateur sur Internet,
- protéger les appareils par plusieurs niveaux de cyberdéfense (pare-feu, détection d'intrusion…),
- séparer le réseau de l'entreprise du réseau de technologie opérationnelle (OT),
- mettre en place une liste d'adresses autorisées.

L'accès par communication Modbus-TCP au disjoncteur hw+ permet d'accéder à toutes ses données d'état, d'indicateurs, de mesure, aux paramètres de réglage et aux fonctions de contrôle à distance.
Les protocoles utilisés sont :
- SNTP : synchronisation de la date et l'heure
- DHCP : affectation d'adresse réseau IP
- DNS : résolutions des noms de domaines
- HTTPS : pour l'accès par Ethernet aux page Web de configuration du module
- Modbus Messaging on TCP/IP : pour la communication du serveur avec les clients Modbus.

Le module de communication Modbus-TCP permet de connecter le serveur disjoncteur hw+ à plusieurs clients ou de connecter un ordinateur par Ethernet pour paramétrer la communication modbus.

Voici nos recommandations pour se prémunir de tout acte malveillant ou involontaire par communication Modbus-TCP :

Concernant un ordinateur connecté par Ethernet au module Modbus-TCP, celui-ci doit être doté d'un antivirus installé, actif et à jour. Il doit être configuré pour fonctionner par session (Identifiant + mot de passe). Les politiques de mots de passe et d'utilisations de l'ordinateur doivent être respectées.
Cet ordinateur doit être attribué uniquement aux personnes habilitées et autorisées.

Concernant la communication avec un client Modbus, si celui-ci et le système de communication déployé le permettent, il est recommandé d'activer le modbus sécurisé par TLS sur le module de communication Modbus-TCP.
Par défaut, le protocole Modbus-TCP n'est pas sécurisé, certains messages peuvent être déchiffrés facilement.

Le module Modbus-TCP permet d'activer le protocole modbus sécurisé avec TLS non authentifié ou bien le protocole Modbus sécurisé avec TLS et authentification mutuelle.

La connexion d'un ordinateur par Ethernet au module de communication permet d'accéder par HTTPS aux pages Web du module pour configurer la stratégie d'affection d'adresse IP et la gestion des certificats X.509 d'authentification du serveur Modbus et de ses clients.

Pour plus d'information sur le modbus sécurisé par TLS et la connexion par HTTPS et se reporter au Guide utilisateur Communication Modbus sentinel Energy.

L'accès par communication Modbus-RTU au disjoncteur hw+ permet d'accéder à toutes ses données d'état, d'indicateurs, de mesure, aux paramètres de réglage et aux fonctions de contrôle à distance.

Voici nos recommandations pour se prémunir de tout acte malveillant ou involontaire par communication Modbus-RTU :

- un logiciel antivirus doit être installé sur l'ordinateur ayant accès au réseau connecté à la communication Modbus-RTU,
- cet antivirus doit être actif et à jour,
- cet ordinateur doit être configuré pour fonctionner par session (identifiant + mot de passe),
- les politiques de mots de passe et d'utilisations de l'ordinateur doivent être respectées,
- cet ordinateur ne doit être attribué qu'aux personnes habilitées et autorisées. .

Pour plus d'information sur l'utilisation du modbus-RTU se reporter au Guide utilisateur Communication Modbus sentinel Energy.

Mise à jour du logiciel Hager Power setup et de l'application Hager Power touch
Il est important de toujours disposer des dernières versions logicielles. En effet, celles-ci en plus de contenir des évolutions et des corrections fonctionnelles, embarquent également des mises à jour de sécurité car les techniques de cyberattaque et de cyberdéfense sont en perpétuelle évolution.

Voici comment mettre à jour les éléments suivants :
- logiciel Hager Power setup : pour être informé d'une mise à jour disponible, l'ordinateur exécutant le logiciel doit être connecté à Internet,
- application Hager Power touch : comme toutes les applications de téléphones mobiles, les mises à jour sont mises à disposition sur Apple store et sur Google Play.

Mise à jour des firmwares
Pour la mise à jour des firmwares du déclencheur sentinel Energy, des modules de communication et de l'afficheur déporté, si une mise à jour est nécessaire, elle sera réalisée par un intervenant Hager.

Assistance à la cybersécurité
Hager a mis en place une politique de gestion des vulnérabilités afin de répondre rapidement aux incidents de faille de cybersécurité sur ses produits et services connectés.

Pour déclarer un incident ou une vulnérabilité de cybersécurité vous pouvez appliquer une des méthodes suivantes :
a) De préférence pour une meilleure réactivité, adresser un courrier à notre équipe Product Security Team en précisant la description du problème ainsi que les références des produits concerné. Courrier électronique à adresser à : productsecurity@hagergroup.com
b) Contacter votre représentant Hager ou l'assistance technique locale Hager (coordonnées sur le site internet Hager de votre pays) en précisant qu'il s'agit d'un problème de cybersécurité, la description du problème ainsi que les références des produits concernés.

La déclaration d'un incident de cybersécurité permet à l'équipe Product Security Team d'évaluer les risques, de proposer des contre-mesures et de faire évoluer les logiciels et matériels en y apportant les corrections nécessaires.

AES
Advanced Encryption Standard

DHCP
Dynamic Host Configuration Protocol. Protocole de Configuration Dynamique d'Hôte utilisé pour la gestion des adresses IP.

DNS
Domaine Name System. Le DNS permet d'associer un nom compréhensible à une adresse IP.

CIP
Communication Interface Port. Se dit également du protocole propriétaire permettant d'interfacer les composants du système sentinel Energy.

ICS
Industrial Control System. Un système de contrôle industriel désigne les objets physiques et numériques, qui régulent et gèrent le comportement des machines et des processus de machines dans les installations industrielles.

MAC
L'adresse MAC (Media Access Control) est l'adresse physique d'un périphérique réseau. Chaque adresse MAC est unique et permet ainsi d'identifier les appareils électroniques.

OT
La technologie opérationnelle (Operational Technology en anglais) est constitué du matériel et du logiciel, qui surveillent, contrôlent les processus et les dispositifs physiques industriels.

RTU
Modbus RTU (Remote Terminal Unit), est un protocole série Open Source issu de la conception maître / esclave initialement créé par Modicon (actuellement Schneider Electric).

SNTP
Simple Network Time Protocol. Se dit d'un serveur chargé de gérer la date et l'heure du réseau de communication.

TCP
Transmission Control Protocol. TCP/IP est un ensemble de règles normalisées permettant aux ordinateurs de communiquer sur un réseau tel qu'Internet.

TLS
Transport Layer Security.

Hager Electro SAS
132 Boulevard d'Europe
BP3
67210 OBERNAI CEDEX

www.hager.com

2023-12

6LE009347A