Leitfaden zur Cybersicherheit

hw+

Leistungsschalter sentinel Energy

HW1, HW2 und HW4

hager

Inhalt

Seite

Warnhinweise und Anmerkungen

Diese Dokumentation enthält Sicherheitshinweise, die Sie für Ihre eigene Sicherheit oder zur Vermeidung von Sachschäden einhalten müssen.
Sicherheitshinweise, die auf eine Gefahr für Ihre persönliche Sicherheit hinweisen, werden in dieser Dokumentation mit einem Sicherheitsalarmsymbol gekennzeichnet. Sicherheitshinweise zur Vermeidung von Sachschäden werden mit „ACHTUNG“ gekennzeichnet.
Die Sicherheitshinweise werden entsprechend der unten aufgeführten Klassifizierung entsprechend ihres Risikos unterteilt.

GEFAHR

GEFAHR weist auf eine unmittelbar bevorstehende Gefahrensituation hin, die, sofern sie nicht vermieden werdn kann, zu schweren Verletzungen bis hin zum Tod führen kann.

WARNHINWEIS

WARNHINWEIS weist auf eine potenziell gefährliche Situation hin, die, sofern sie nicht vermieden werden kann, zu schweren Verletzungen einschließlich zum Tod führen kann.

VORSICHT

VORSICHT weist auf eine Situation hin, die unter Umständen Gefahren bergen kann, die zu leichten bis mittelschweren Verletzungen führen können, wenn sie nicht vermieden werden.

ACHTUNG

ACHTUNG entspricht einer Warnung vor eventuellen Sachschäden.
ACHTUNG weist ebenfalls auf wichtige Nutzungshinweise und vor allem nützliche Produktinformationen hin, denen für den effizienten und sicheren Einsatz besondere Aufmerksamkeit gewidmet werden sollte.

Qualifiziertes Personal

Das in dieser Dokumentation beschriebene System oder Produkt darf nur von qualifiziertem Personal installiert, betrieben und instandgehalten werden. Hager Electro weist jegliche Verantwortung für durch die Nutzung dieses Materials durch nicht qualifiziertes Personal entstandene Schäden entschieden zurück.
Qualifiziertes Personal sind Personen, die über die für den Aufbau und Betrieb von Anlagen mit elektronischen Geräten erforderliche Kompetenz und über entsprechende Kenntnisse verfügen und die eine Ausbildung absolviert haben, die es ihnen ermöglicht, eventuelle Risiken zu beurteilen und zu vermeiden.

Zweckmäßiger Einsatz der Produkte von Hager

Die Produkte von Hager sind ausschließlich für die in den Katalogen und in der jeweiligen technischen Dokumentation beschriebenen Zwecke bestimmt. Sollten Produkte und Komponenten von anderen Herstellern zum Einsatz kommen, müssen diese von Hager empfohlen oder genehmigt sein.
Zur Gewährleistung eines sicheren und reibungslosen Betriebs ist ein angemessener Umgang der Produkte von Hager bei Transport, Lagerung, Installation, Montage, Inbetriebnahme, Betrieb und Instandhaltung unerlässlich.
Die zulässigen Umgebungsbedingungen sind einzuhalten. Die in der technischen

Dokumentation enthaltenen Informationen sind zu berücksichtigen

Haftungsansprüche aufgrund der Veröffentlichung

Der Inhalt dieser Dokumentation wurde zur Gewährleistung der Richtigkeit der darin enthaltenen Informationen zum Zeitpunkt der Veröffentlichung geprüft.
Hager kann jedoch nicht gewährleisten, dass sämtliche in dieser Dokumentation enthaltenen Informationen korrekt sind. Hager weist jegliche Verantwortung für Druckfehler und sich daraus ergebende Schäden entschieden zurück.
Hager behält sich das Recht vor, eventuell erforderliche Korrekturen und Änderungen in späteren Ausgaben einzubringen.

Cybersicherheit und drahtlose Verbindung

Das in dieser Dokumentation beschriebene Produkt oder System erfordert die Ergreifung von Schutzmaßnahmen gegen die Gefahren, die von jeder drahtlosen Verbindung und Übertragung ausgehen, sowie gegen die Gefahren jeder drahtgebundenen Verbindung und Übertragung.

⚠ WARNHINWEIS

Gefahren von Hackerangriffen über drahtlose Verbindung
- Die Bluetooth Low Energy-Verbindung deaktiviert lassen, wenn die App Hager Power touch nicht mehr verwendet wird.
- Die Aktivierung der Bluetooth Low Energy-Verbindung vermeiden, wenn nicht jeder unbefugte Zugriff auf die installierten Geräte unterbunden werden kann.

Nichtbeachtung dieser Anweisungen kann Todesfälle oder schwere Verletzungen oder Sachschäden zur Folge haben.

⚠ WARNHINWEIS

Mögliche Gefahren für Verfügbarkeit, Integrität und Vertraulichkeit des Systems sentinel Energy
- Ändern Sie Passwörter standardmäßig bei der ersten Benutzung, um jeden unbefugten Zugriff auf die Einstellungen, Steuerungen und Informationen der Geräte zu verhindern.
- Deaktivieren Sie standardmäßig nicht genutzte Ports, Dienste und Konten, um die Gefahr böswilliger Angriffe zu verringern.
- Schützen Sie Netzwerkgeräte durch mehrere Verteidigungsebenen gegen Cyberangriffe (Firewall, Segmentierung des Netzwerks, Erkennung von Eindringlingen (Intrusion Detection) und Schutz des Netzwerks).
- Beachten Sie die bewährten Vorgehensweisen der Cybersicherheit (zum Beispiel: nur erforderlicher Mindestumfang an Berechtigungen, Aufgabentrennung), um die Gefahren durch Eindringlinge, Verlust oder Veränderung von Daten und Protokollen oder die Unterbrechung der Dienste zu verringern.

Nichtbeachtung dieser Anweisungen kann Todesfälle oder schwere Verletzungen oder Sachschäden zur Folge haben.

Gegenstand des Dokuments

Dieses Dokument soll Elektroinstallateuren, Systemintegratoren oder Systementwicklern die Cybersicherheitselemente von Leistungsschaltern hw+ mit elektronischen Auslöseeinheiten sentinel Energy vermitteln. Dies soll den Entwicklern und Benutzern dieser Systeme helfen, eine sichere Umgebung für den Betrieb des Produkts zu implementieren.

Anwendungsbereich

Dieses Dokument gilt für Leistungsschalter hw+, die mit elektronischen Auslöseeinheiten sentinel Energy ausgestattet sind.

Revisionen

Index	Datum
6LE009348A	Dezember 2023

Zugehörige Dokumente

Dokument	Referenz
HW1-Installationshandbuch	6LE007890A
Installationshandbuch HW2 und HW4	6LE009213A
Benutzerhandbuch für elektronische Auslöseeinheiten sentinel Energy hw+	6LE008148A
Benutzerleitfaden für die Modbus-Kommunikation von sentinel Energy	6LE007965A

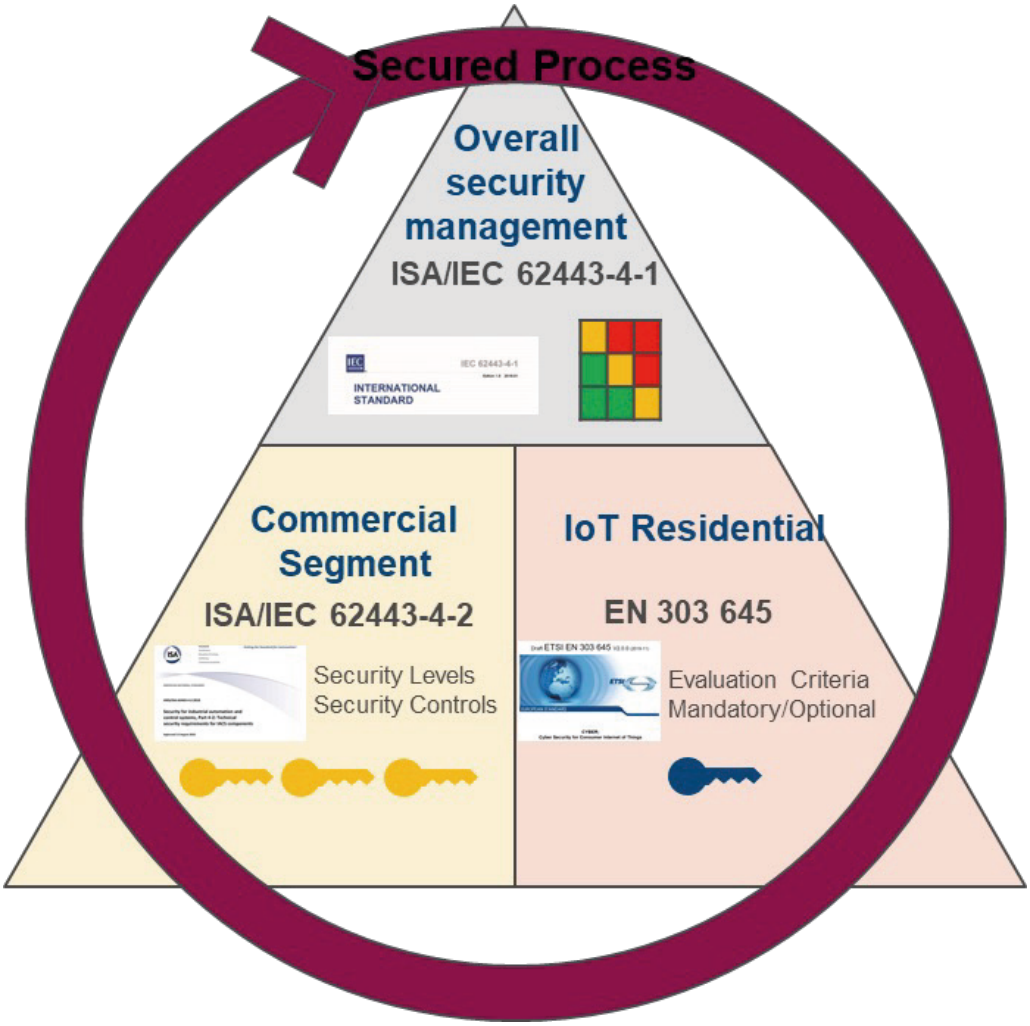
Diese Veröffentlichungen und weitere technische Informationen können Sie von unserer Website www.hager.com herunterladen.

Kontakt

Adresse	Hager Electro SAS, 132 Boulevard d'Europe, 67215 Obernai, Frankreich
Telefon	+ 33 (0)3 88 49 50 50
Website	www.hager.com

Hager legt besonderen Wert auf Datenschutz und Sicherheit der Verbindung für seine vernetzten Produkte.
Deshalb unternehmen wir alle Anstrengungen, um die höchsten Qualitätsstandards in Bezug auf die Sicherheit der Daten, die durch unsere Produkte transportiert werden, zu erreichen.

Hager verwendet die Normen IEC 62443 und EN 303 645 bei der Entwicklung seiner vernetzten Produkte.
Die Norm IEC 62443 gilt für den sicheren Betrieb von industriellen Automatisierungssystemen (ICS-Systemen), von der Planung über die Implementierung bis hin zur Verwaltung.
Die Norm EN 303 645 definiert auf hohem Niveau geltende Cybersicherheits- und Datenschutzbestimmungen für vernetzte IoT-Geräte für Verbraucher.



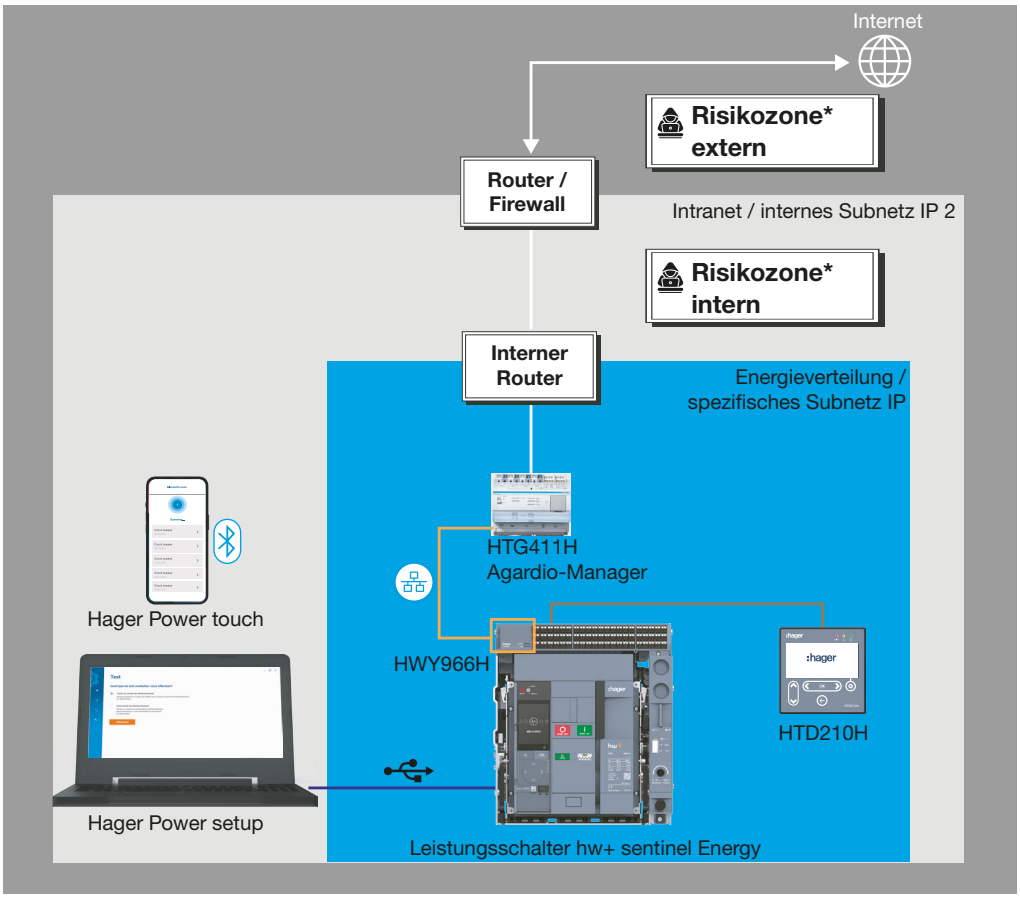
Die Anwendung eines sicheren Verfahrens während der Entwurfs-, Entwicklungs- und Validierungsphase verhindert auch Angriffe, die darauf abzielen, Ihre Produkte zu stören oder die Konfiguration Ihres Systems zu ändern.

2.2.1 Umgebung des Systems sentinel Energy

Der Leistungsschalter hw+ sentinel Energy ist ein wichtiger Bestandteil für die Elektroverteilung und die nachgeschalteten Betriebsmittel, da er einen elektrischen Schutz bietet.

Mit seinen Kommunikationsfunktionen bietet er Zugriff auf Echtzeit-Steuerfunktionen und auf Überwachungsdaten zur Energieverteilung. Dies ermöglicht eine höhere Effizienz und Flexibilität bei der Verwaltung Ihrer elektrischen Anlage. Diese Funktionen werden jedoch potenziellen Cyberangriffen ausgesetzt.

Die folgende Abbildung zeigt die Kommunikationsumgebung, in die der Leistungsschalter hw+ sentinel Energy integriert ist.



Legende:

	Internet
	Intranet
	Verteilschrank
	Modbus-Kommunikation
	USB-C
	CIP-Port für proprietäres Protokoll
	Bluetooth Low Energy

(*) Risiko von Angriffen oder Kompromittierungen

Das Eco-System sentinel Energy hat verschiedene Schnittstellen die durch die über verschiedene Kommunikationsmedien mit dem Leistungsschalter hw+ interagieren, wie folgt:
- über die Schnittstelle Display/Tastatur der Auslöseeinheit sentinel Energy,
- über die kabellose Verbindung Bluetooth Low Energy (BLE) von einem Smartphone mit der App Hager Power touch,
- über den USB-C-Anschluss zur Software Hager Power setup,
- über eine serielle Verbindung mit dem proprietären CIP-Protokoll zum Türeinbau-Display HTD210H,
- über die Verbindung zu einem RS 485-Serial-Link-Netzwerk mithilfe des Modbus-RTU-Protokolls,
- über die Verbindung zu einem Ethernet-Netzwerk mithilfe des Modbus-TCP-Protokolls.

Jedes dieser Kommunikationsmedien stellen an den Schnittstellen eine Schwachstelle für einen potentiellen Angriff auf das ganze System dar.
Werden keine geeignete Sicherheitsmassnahmen dagegen ergriffen werden, ist ihr System den folgenden Risiken ausgesetzt:
- Risiko eines Ausfalls des Systems und somit ein Blackout,
- Risiko einer Änderung der Systemparametern durch unbefugte Personen und somit ist der Schutz oder keine Kommunikation mehr gewährleistet.
- Risiko der Übernahme und der Kontrolle des ganzen Gebäudemanagementsystems durch Unbefugte und somit einen Cyberangriff entspricht,
- Risiko des Verlusts kritischer und sensibler Daten und somit Teil eines Cyberangriffs entspricht.

Dieser Leitfaden enthält unsere Empfehlungen zur Sicherung dieser Kommunikationsmittel und zur Vermeidung von vorsätzlichen Angriffen oder versehentlichem Missbrauch.

2.2.2 Sicherheitsfunktionen

Die folgenden Sicherheitsfunktionen wurden bei der Planung integriert, um die Gefahren entgegen zu wirken, die mit dem Einsatz der sentinel Energy-Anlage in einer vernetzten Umgebung einhergehen:

- Sicherung der Bluetooth-Kommunikation mit dem AES-Algorithmus,
- Aktionen zur Änderung von Einstellungen und Steuerungs-/Befehlsaktionen erst nach Eingabe von Passwörtern oder benutzerdefinierten Codes möglich,
- Verschlüsselte IP-Kommunikation,
- Aktivierung der Verschlüsselung und Authentifizierung der Modbus-Kommunikation,
- Einstufung der Sicherheitsstufe beim Schreiben von Befehlen in die Modbus-Register.

Diese Sicherheitsfunktionen sowie die Funktionsweise des sentinel Energy Eco-Systems wurden von externen und unabhängigen Drittorganisationen im Rahmen von Penetrationstests (Simulation von Angriffen durch einen böswilligen Benutzer oder Malware) getestet und validiert.

Operative Technologie (OT) bezieht sich auf die Hardware und Software, die zur Überwachung physischer Geräte und Prozesse innerhalb eines Unternehmens verwendet werden. Während ihres Einsatzes ist es wichtig, Daten zu identifizieren und zu schützen, die für den Betrieb eines Unternehmens kritisch oder sensibel sind.

Sensible Daten sind beispielsweise:
- Zugangscodes für verschlossene Ausrüstungsgegenstände oder Räume,
- Systemarchitektur,
- IP- oder MAC-Adressen der vernetzten Kommunikationsgeräte,
- die für die Ethernet-Kommunikation verwendeten Portnummern,
- Benutzer-IDs und Passwörter.

Hinzu kommen die Informationen, die von der sentinel Energy Eco-System geliefert werden.

	Display sentinel Energy	**Türeinbau-Display HTD210H**	**Bluetooth**	**USB-C**	**Modbus RTU Modbus TCP**
Modbus TCP					
Datenüberwachung	Lesen	Lesen	Lesen	Lesen	Lesen
Schutzparameter des Leistungsschalters	Lesen/ Schreiben	Lesen/ Schreiben	Lesen	Lesen/ Schreiben	Lesen/ Schreiben
Andere Einstellungen des Leistungsschalters	Lesen/ Schreiben	Lesen/ Schreiben	Lesen	Lesen/ Schreiben	Lesen/ Schreiben
Befehle zum Aus- und Einschalten	Ja	Keine (none)	Ja	Ja	Ja
Zurücksetzen	Ja	Ja	Keine (none)	Ja	Ja

Einer der wichtigsten Punkte einer Abwehrstrategie gegen Cyberangriffe ist die Durchsetzung einer effektiven Passwortrichtlinie.

⚠ WARNHINWEIS

Mögliche Gefahren für Verfügbarkeit, Integrität und Vertraulichkeit des Systems sentinel Energy
Ändern Sie Passwörter standardmäßig bei der ersten Benutzung, um jeden unbefugten Zugriff auf die Einstellungen, Steuerungen und Daten der Geräte zu verhindern. Nichtbeachtung dieser Anweisungen kann Todesfälle oder schwere Verletzungen oder Sachschäden zur Folge haben.

Dies umfasst die folgenden bewährten Verfahren (nicht erschöpfende Auflistung):
- Ändern aller Standardpasswörter
- Festlegung starker Passwörter: Triviale Passwörter wie „1234“ oder „Passwort“ müssen vermieden werden.
- Keine Weitergabe von Passwörtern an unbefugte oder nicht berechtigte Personen
- Regelmäßige Änderung von Passwörtern
- Keine Wiederverwendung von alten Passwörtern
- Speicherung der Passwörter an einem sicheren Ort (z. B. in einem Passwortspeicher)

Diese Passwortrichtlinie muss auf alle Systemkomponenten von sentinel Energy, Servern, Computern, Smartphones, die mit dem System verbunden sind, und alle anderen Netzwerkkomponenten angewendet werden.

Cybersicherheit betrifft alle Mitarbeiter des Unternehmens. Insbesondere müssen alle Nutzer, die auf die sentinel Energy Eco-System und das Kommunikationsnetzwerk der Anlage zugreifen dürfen, die Strategie zum Schutz der Informationen des Unternehmens kennen.

Darüber hinaus müssen sie eine Schulung zu den Grundlagen der Cybersicherheit und den sich aus dieser Strategie ergebenden Umsetzungsvorschriften erhalten haben.

Es ist notwendig, regelmäßig auf die folgenden bewährten Verfahren (und nicht nur auf diese) hinzuweisen:

- Befolgen der Passwortrichtlinie,

keine Weitergabe von Passwörtern, Zugangscodes und vertraulichen Daten,

- Gewährleistung, dass alle an das System angeschlossenen Computer (Inbetriebnahme, Überwachung, Steuerung usw.) auf dem neuesten Stand und vor Viren und Malware geschützt sind,
- Schulung der Anwender in der Erkennung verdächtiger E-Mails, wenn die Computer auch für den Nachrichtenversand verwendet werden,
- Schutz aller Smartphones, die für den Zugriff auf das System verwendet werden, vor Hackerangriffen im Internet und über Bluetooth durch einen PIN-Code oder eine Gesichtserkennung,
- Erhalt der Systemintegrität sowie der Komponenten aller Smartphones,
- durchgängiger Verbleib aller Smartphones, die für den Zugriff auf das System verwendet werden, im Besitz von Benutzern - keine Nutzung durch Andere,
- keine Umgehung bestehender Sicherheitsrichtlinien.

Der Nahzugriff auf den in den Leistungsschalter hw+ integrierten Auslöser sentinel Energy ermöglicht den Zugriff auf alle seine Funktionen, insbesondere seine Schutz- und Einstellungen für den Fernzugriff.

Daher ist es wichtig, den Zugang zu beschränken, indem der Leistungsschalter in einem verschlossenen oder durch einen Zugangscode geschützten Raum installiert wird, um Folgendes zu vermeiden:

- jeden unbefugten Zugriff auf das Display sentinel Energy und die entsprechende Tastatur, um das Risiko einer Änderung der Einstellungs- und Steuerungsparameter zu vermeiden;
- jeden unbefugten Zugriff auf die drahtlose Bluetooth-Kommunikation, um das Risiko einer Übernahme der Kontrolle über die App Hager Power touch zu vermeiden;
- jede nicht autorisierte Verbindung über den USB-C-Port, um das Risiko einer Änderung der Parameter der Software Hager Power setup zu vermeiden.

Insbesondere muss Folgendes überprüft werden:

- dass der Raum stets abgeschlossen ist,
- dass der Raum mit einem Authentifizierungs- und Autorisierungssystem ausgestattet ist,
- dass nur autorisiertes Personal über einen Schlüssel oder Zugangscode verfügt,
- dass die Kommunikationskabel, die in den Raum führen, und die Anschlüsse an Kommunikationsgeräten außerhalb des Raums geschützt sind,
- dass alle Geräte (Computer, Smartphones und Tablets), die Zugriff auf die Auslöseeinheit sentinel Energy haben, über einen besseren Schutz gemäß den aktuellen Anweisungen des Lieferanten verfügen.

Jede Person, die einen Zugang zum Schaltschrank hat wo der Leistungsschalter hw+ installiert ist, hat Zugriff auf das Display sentinel Energy sowie die entsprechende Tastatur und kann somit die Einstellparameter des Leistungsschalter ändern.

Um einen Schutz vor böswilligen oder unbeabsichtigten Handlungen beim Zugriff auf die Tastatur und das Display des sentinel Energy, empfehlen wir folgende Aktionen:

- Passwortschutz für die Änderung aller Parameter aktivieren (mit Ausnahme der Parameter zum Einstellen des Anzeigebildschirms),
- Tastatursperre von sentinel Energy aktivieren,
- die transparente Abdeckung des Schutzes der Auslöseeinheit verplomben,
- Passwort für den Auslöser sentinel Energy nur an autorisierte Personen weitergeben,
- keine Speicherung des Passwortes auf dem Smartphone, auf dem die App Hager Power touch installiert ist (SMS, E-Mail, Notizen usw.).

Über ein Smartphone, dass über die App "Hager Power touch" verfügt und über Bluetooth mit der Auslöseeinheit sentinel Energy verbunden ist, können Daten ausgelesen oder den Leistungsschalter hw+ Ein- bzw. Ausgeschaltet oder Ausgelöst werden.

Um einen Schutz vor böswilligen oder unbeabsichtigten Handlungen durch Zugriff über die Bluetooth-Verbindung, empfehlen wir folgende Aktionen:

- Installation des Leistungsschalters hw+ in einem Raum, der stets verschlossen ist oder der jederzeit über einen Zugangsschutz verfügt,
- nur befugte Personen haben Zugang zu dem Raum,
- das Kennwort für die Auslöseeinheit sentinel Energy darf nur autorisierten Personen mitgeteilt werden.

Nutzung der App Hager Power touch

Mit der App Hager Power touch App können die vom Auslöser sentinel Energy gelieferten Informationen überwacht werden, insbesondere der Betriebszustand des Leistungsschalters und die gemessenen Messgrössen.
Die App ermöglicht auch die Ausführung eines Befehls zum Öffnen und Schließen des Leistungsschalters hw+, wenn das entsprechende Zubehör am Leistungsschalter installiert wurde.

Bei der ersten Verbindung erfordert die Kopplung des Smartphones, auf dem die App Hager Power touch ausgeführt wird, mit dem Leistungsschalter eine physische Aktion an der Auslöseeinheit sentinel Energy. Ab der zweiten Verbindung ist keine Kopplung mehr erforderlich. Die Verbindung mit dem Smartphone wird automatisch hergestellt, wenn die Bluetooth-Kommunikation aktiviert ist und sich das Gerät innerhalb der Reichweite von Bluetooth Low Energy befindet.
Weitere Informationen dieser App finden Sie im Benutzerhandbuch für elektronische Auslöseeinheiten sentinel Energy hw+.

Daher ist es unerlässlich, dass durch die Bluetooth-Kommunikation mit der App Hager Power touch jedes Risiko von Hackerangriffen vermieden wird.

⚠ WARNHINWEIS

Gefahren von Hackerangriffen über drahtlose Verbindung

- Lassen Sie die Verbindung Bluetooth Low Energy der Auslöseeinheit deaktiviert, wenn die App Hager Power touch nicht von Ihrer IT-Abteilung genehmigt wurde.
- Deaktivieren Sie die Verbindung Bluetooth Low Energy der Auslöseeinheit, wenn die App Hager Power touch längere Zeit nicht verwendet wird.
- Entfernen Sie ihr gespeicherte Gerätezugang "hw+-Leistungsschalter" von Ihren Bluetooth-Einstellungen in Ihrem Smartphone, wenn die Hager Power touch App für längere Zeit nicht verwendet wird.
- Vermeiden Sie die Aktivierung der Verbindung Bluetooth Low Energy der Auslöseeinheit, wenn Sie nicht in der Lage sind, jeden unbefugten Zugriff auf die installierten Geräte zu unterbinden.

Nichtbeachtung dieser Anweisungen kann Todesfälle oder schwere Verletzungen oder Sachschäden zur Folge haben.

Durch die Verbindung mit dem USB-C-Port mithilfe der Software Hager Power setup können Sie auf die Schutz- und Steuerfunktionen der Auslöseeinheit sentinel Energy zugreifen.

⚠ WARNHINWEIS

Mögliche Gefahren für Verfügbarkeit, Integrität und Funktion des Systems sentinel Energy
Verplomben Sie die transparente Abdeckung der Auslöseeinheit, wenn Sie nicht in der Lage sind, unbefugten Zugriff auf den Leistungsschalter zu verhindern.
Nichtbeachtung dieser Anweisungen kann Todesfälle oder schwere Verletzungen oder Sachschäden zur Folge haben.

Um eine Verbindung mit dem USB-C-Port herzustellen, müssen die folgenden Bedingungen erfüllt sein:
- Physischer Zugriff auf die USB-C-Buchse an der Auslöseeinheit sentinel Energy,
- die Software Hager Power setup muss auf einem Laptop installiert sein,
- dieser Computer muss über einen USB-C-Adapter an der Auslöseeinheit angeschlossen sein.

Folgen Sie der folgenden Empfehlungen bei der Verwendung der Software Hager Power setup:

Es gibt viele Angriffe, die Sicherheitslücken im Microsoft Windows-Betriebssystem ausnutzen. Aus diesem Grund muss der Computer, auf dem Hager Power setup installiert ist, gesichert werden:
- auf dem Computer muss eine Virenschutzsoftware installiert, aktiv und auf dem neuesten Stand sein,
- der Computer muss für den Betrieb pro Sitzung konfiguriert werden (ID und Passwort),
- die Richtlinien zu Passwörtern und zur Computernutzung müssen eingehalten werden,
- die Software Hager Power setup muss über die neuesten Updates verfügen.

Das Türeinbau-Display HTD210H bietet Zugriff auf verschiedene Funktionen der Auslöseeinheit, einschließlich der Schutzeinstellungen.

Daher ist es wichtig, den Zugang zu beschränken, indem der Leistungsschalter in einem verschlossenen oder durch einen Zugangscode geschützten Raum installiert wird, um Folgendes zu vermeiden:

- jeden unbefugten Zugriff auf das Display sentinel Energy und die entsprechende Tastatur, um das Risiko einer Änderung der Einstellungs- und Steuerungsparameter zu vermeiden;
- jeden unbefugten Zugriff auf die drahtlose Bluetooth-Kommunikation, um das Risiko einer Übernahme der Kontrolle über die App Hager Power touch zu vermeiden;
- jede nicht autorisierte Verbindung über den USB-C-Port, um das Risiko einer Änderung der Parameter der Software Hager Power setup zu vermeiden.

Insbesondere muss Folgendes überprüft werden:

- der Raum ist stets abgeschlossen,
- der Raum ist mit einem Authentifizierungs- und Autorisierungssystem ausgestattet,
- nur autorisiertes Personal hat einen Schlüssel oder Zugangscode.

Befolgen Sie unsere folgende Empfehlungen, um sich vor böswilligen oder unbeabsichtigten Handlungen durch Zugriff auf das Türeinbau-Display HTD210H zu schützen:

- Änderung des Passworts für den Zugriff auf das Türeinbau-Display HTD210H bei der ersten Verwendung,
- Aktivierung der Tastatursperre des Displays,
- Verplomben der transparenten Abdeckung der Auslöseeinheit,
- Passwortweitergabe für das Display nur an autorisierte Personen.

Der mit einem Auslöser sentinel Energy ausgestattete Leistungsschalter hw+ bietet zwei Möglichkeiten für den Fernzugriff:
- über ein Netzwerk mit serieller RS-485-Schnittstelle mithilfe des Modbus-RTU-Protokolls beim Kommunikationsmodul HWY965H,
- über ein Ethernet-Netzwerk mithilfe des Modbus-TCP/IP-Protokolls beim Kommunikationsmodul HWY966H.

Dieser Fernzugang ermöglicht den Zugriff auf alle Funktionen der Auslöseeinheit sentinel Energy, einschließlich Schutz und Fernsteuerungseinstellungen.

Es ist daher wichtig, die Fernzugriffssperre zu aktivieren, wenn der Schreibzugriff auf die Parameter des Auslösers und der Zugriff auf die Steuerfunktionen aus der Ferne nicht erforderlich sind.

Die Fernzugriffssperre erfolgt über den Auslöser sentinel Energy.
Weitere Informationen finden Sie im Benutzerhandbuch für elektronische Auslöseeinheiten sentinel Energy hw+.

Um diesen Zugang abzusichern, empfehlen wir Folgendes:
- keine Portweiterleitung am Modem-Router vornehmen. Dadurch würde Ihre Modbus-Schnittstelle oder Ihr Konfigurator im Internet zugänglich,
- die Geräte durch mehrere Ebenen der Cyberabwehr (Firewall, Intrusion Detection usw.) schützen,
- Trennung des Unternehmensnetzes vom Netz der operativen Technologie (OT),
- Erstellen einer Liste autorisierter Adressen.

Der Zugang mit Hilfe der Kommunikation über Modbus-TCP auf den Leistungsschalter hw+ ermöglicht den Zugriff auf alle Status-, Anzeige- und Messdaten, Einstellparameter und Fernsteuerungsfunktionen.
Folgende Protokolle werden verwendet:
- SNTP: Synchronisierung von Datum und Uhrzeit
- DHCP: Zuweisung der IP-Netzwerkadresse
- DNS: Auflösung von Domänennamen
- HTTPS: für den Ethernet-Zugriff auf die Website der Modulkonfiguration
- Modbus Messaging auf TCP/IP: für die Serverkommunikation mit Modbus-Clients.

Der Modbus-TCP-Schaltaufsatz ermöglicht es, den Leistungsschalter-Server hw+ mit mehreren Clients zu verbinden oder einen Computer über Ethernet anzuschließen, um die Modbus-Kommunikation einzurichten.

Folgen Sie der folgenden Empfehlungen bei zum Schutz vor böswilligen oder unbeabsichtigten Handlungen durch die Modbus-TCP-Kommunikation:

Auf einem Computer, der über Ethernet mit dem Modbus-TCP-Modul verbunden ist, muss eine Virenschutzsoftware installiert, aktiv und auf dem neuesten Stand sein. Er muss für den Betrieb pro Sitzung konfiguriert sein (ID und Passwort). Die Richtlinien zu Passwörtern und zur Computernutzung müssen eingehalten werden.
Dieser Computer darf nur befugten und autorisierten Personen zugewiesen werden.

In Bezug auf die Kommunikation mit einem Modbus-Client wird empfohlen, den TLS-gesicherten Modbus auf dem Modbus-TCP-Kommunikationsmodul zu aktivieren, wenn der Modbus-Client und das eingesetzte Kommunikationssystem dies zulassen.
Standardmäßig ist das Modbus-TCP-Protokoll nicht gesichert. Einige Nachrichten können einfach entschlüsselt werden.

Mit dem Modbus-TCP-Modul können Sie das gesicherte Modbus-Protokoll mit nicht authentifiziertem TLS oder das gesicherte Modbus-Protokoll mit TLS und gegenseitiger Authentifizierung aktivieren.

Das Anschließen eines Computers über Ethernet an das Kommunikationsmodul ermöglicht den HTTPS-Zugriff auf die Websites des Moduls, um die IP-Adresszuweisungsrichtlinie und die Verwaltung der X.509-Authentifizierungszertifikate für den Modbus-Server und seine Clients zu konfigurieren.

Weitere Informationen zur TLS-gesicherten Modbus- und HTTPS-Verbindung finden Sie im Benutzerleitfaden für die Modbus-Kommunikation von sentinel Energy.

Der Zugang mit Hilfe der Kommunikation über Modbus-RTU auf den Leistungsschalter hw+ ermöglicht den Zugriff auf alle Status-, Anzeige- und Messdaten, Einstellparameter und Fernsteuerungsfunktionen.

Folgen Sie der folgenden Empfehlungen bei zum Schutz vor böswilligen oder unbeabsichtigten Handlungen durch die Modbus-RTU-Kommunikation:

- Auf einem Computer der im Netzwerk den Zugriff auf die Modbus-RTU-Kommunikation hat, muss eine Virenschutzsoftware installiert sein,
- diese muss aktiv und auf dem neuesten Stand sein.
- Der Computer muss für den Betrieb pro Sitzung konfiguriert sein (ID und Passwort).
- Die Richtlinien zu Passwörtern und zur Computernutzung müssen eingehalten werden.
- Dieser Computer darf nur befugten und autorisierten Personen zugewiesen werden. .

Weitere Informationen zur Nutzung von Modbus RTU sind dem Benutzerhandbuch zur Modbus-Kommunikation von sentinel Energy zu entnehmen.

Aktualisierung der Software Hager Power setup und der App Hager Power touch
Es ist wichtig, immer die neuesten Softwareversionen zu haben. Diese umfassen neben funktionalen Entwicklungen und Korrekturen auch Sicherheitsupdates, da sich die Technik von Cyberangriffen und die Abwehrtechniken ständig weiterentwickeln.

So aktualisieren Sie die folgenden Elemente:
- Software Hager Power setup: Um über ein verfügbares Update informiert zu werden, muss der Computer, auf dem die Software ausgeführt wird, mit dem Internet verbunden sein.
- App Hager Power touch: Wie bei allen Apps für Mobiltelefone sind Updates im Apple Store und bei Google Play verfügbar.

Firmware-Aktualisierung
Die Aktualisierung der Firmware der Auslöseeinheit sentinel Energy, der Kommunikationsmodule und des Türeinbau-Displays wird, falls sie erforderlich ist, von einem Hager-Servicetechniker durchgeführt.

Unterstützung bei der Cybersicherheit
Hager hat eine Richtlinie für das Schwachstellenmanagement eingeführt, um schnell auf Vorfälle von Cybersicherheitslücken bei seinen vernetzten Produkten und Dienstleistungen reagieren zu können.

Um einen Cybersicherheitsvorfall oder eine Sicherheitslücke zu melden, können Sie eine der folgenden Methoden verwenden:
a) Um schneller reagieren zu können, schicken Sie am besten ein E-Mail an unser Produktsicherheitsteam, in dem Sie das Problem beschreiben und die Referenzen der betroffenen Produkte angeben. E-Mail an: productsecurity@hagergroup.com
b) Wenden Sie sich an Ihren Hager-Vertreter oder an den technischen Support von Hager vor Ort (Kontaktdaten auf der Hager-Website Ihres Landes), und geben Sie an, dass es sich um ein Cybersicherheitsproblem handelt. Geben Sie außerdem die Beschreibung des Problems und die Bestellnummern der betroffenen Produkte an.

Durch das Melden eines Cybersicherheitsvorfalls kann das Produktsicherheitsteam Risiken einschätzen, Gegenmaßnahmen vorschlagen und Software sowie Hardware mit den erforderlichen Korrekturen aktualisieren.

AES
Advanced Encryption Standard

DHCP
Dynamic Host Configuration Protocol. Dynamisches Host-Konfigurationsprotokoll, das zur Verwaltung von IP-Adressen dient.

DNS
Domain Name System. Mit DNS können Sie einer IP-Adresse einen verständlichen Namen zuordnen.

CIP
Communication Interface Port. Wird auch als proprietäres Protokoll für die Verbindung der Komponenten des Systems sentinel Energy bezeichnet.

ICS
Industrial Control System. Ein industrielles Steuerungssystem bezeichnet die physischen und digitalen Objekte, die das Verhalten von Maschinen und Maschinenprozessen in Industrieanlagen regeln und verwalten.

MAC
Die MAC-Adresse (Media Access Control) ist die physische Adresse eines Netzwerkgeräts. Jede MAC-Adresse ist eindeutig und kennzeichnet somit elektronische Geräte.

OT
Die operative Technologie (Operational Technology) besteht aus Hard- und Software, die industrielle Prozesse und physische Geräte überwachen und steuern.

RTU
Modbus RTU (Remote Terminal Unit) ist ein serielles Open Source-Protokoll aus dem Master/Slave-Design, das ursprünglich von Modicon (jetzt Schneider Electric) entwickelt wurde.

SNTP
Simple Network Time Protocol. Bezeichnet einen Server, der für die Verwaltung von Datum und Uhrzeit des Kommunikationsnetzwerks zuständig ist.

TCP
Transmission Control Protocol. TCP/IP ist eine standardisierte Gruppe von Netzwerkprotokollen, mit denen Computer über ein Netzwerk wie das Internet kommunizieren können.

TLS
Transport Layer Security.

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

www.hager.com

2024-03

6LE009348A