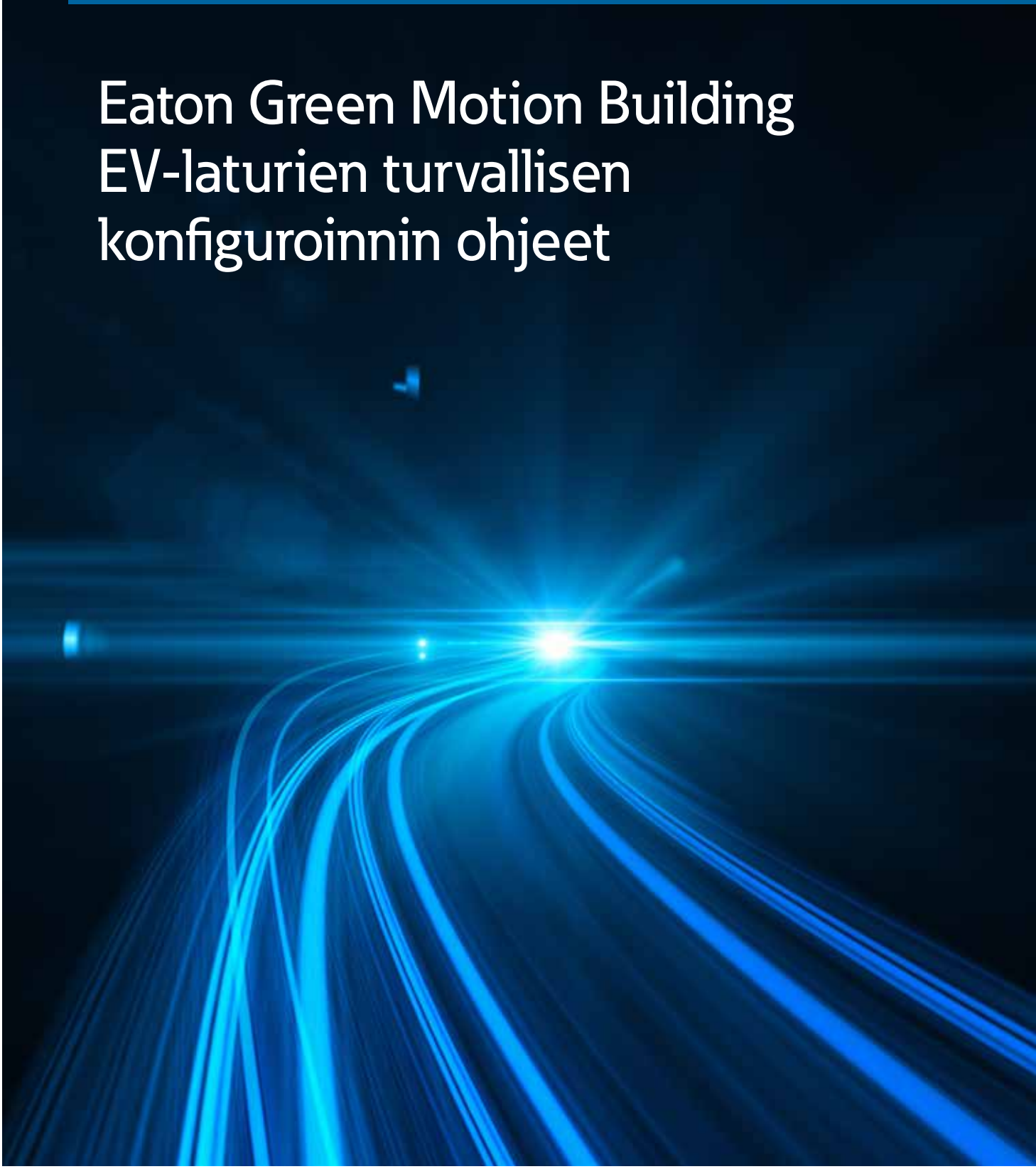
Eatonin kyberturvallisuuden osaamiskeskus
Kyberturvallisuutta koskevat suositukset

Eaton Green Motion Building EV-laturien turvallisen konfiguroinnin ohjeet



Powering Business Worldwide

Dokumentaatio Eatonin tuotteiden turvalliseen käyttöönottoon ja konfigurointiin.

Eaton Green Motion Building EV -latauslaitteen suunnittelussa on kiinnitetty erityistä huomiota kyberturvallisuuteen. Tuotteessa on useita ominaisuuksia kyberturvallisuusriskien torjumiseksi. Näissä kyberturvallisuussuosituksissa annetaan tietoja, joiden avulla käyttäjät voivat ottaa tuotteen käyttöön ja ylläpitää sitä tavalla, joka minimoi kyberturvallisuusriskit. Näiden kyberturvallisuussuositusten tarkoituksena ei ole tarjota kattavaa opasta kyberturvallisuudesta, vaan pikemminkin täydentää asiakkaiden nykyisiä kyberturvallisuusohjelmia.

Eaton on sitoutunut minimoimaan tuotteidensa kyberturvallisuusriskin ja ottamaan käyttöön parhaita kyberturvallisuuskäytäntöjä tuotteissaan ja ratkaisuissaan, mikä tekee niistä entistä turvallisempia, luotettavampia ja kilpailukykyisempiä asiakkaiden kannalta.

Seuraavista dokumenteista on saatavilla lisätietoja yleisistä parhaista kyberturvallisuuskäytännöistä ja -ohjeista:

Sähköisten jakelujärjestelmien kyberturvallisuusnäkökohdat (WP152002EN):

http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Muistutus parhaiden kyberturvallisuuskäytäntöjen tarkistuslistasta (WP910003EN):

https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

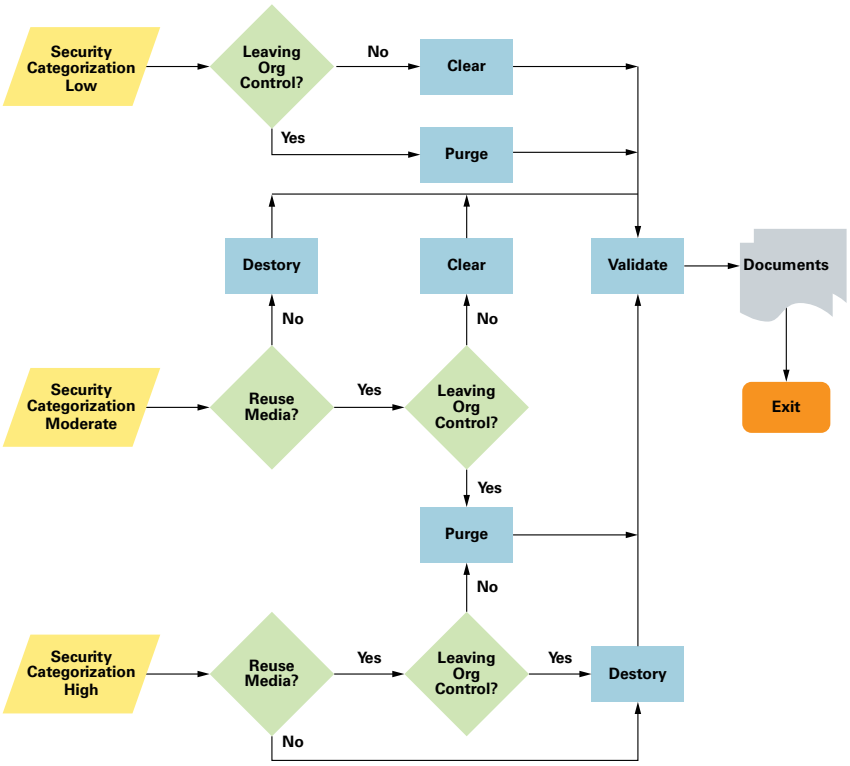
Nykyaikaisten ajoneuvojen tietoverkkoturvallisuuden parhaat käytännöt - NHTSA

https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

Kategoria	Kuvaus
Käyttötarkoitus ja käyttöönottoympäristö	Sovelletaan latureihin, jotka on liitetty Eaton Charging Network Manageriin ohjelmaan (taustalle) tai kolmannen osapuolen liitettyyn tuotteeseen. Käytetään asiakkaiden tiloissa yksityisillä tai julkisilla pysäköintipaikoilla, jotta sähköautojen lataaminen, tunnistautuminen, laskutus jne. on mahdollista. Lisätietoja tuotteen turvallisesta käytöstä, asennuksesta ja käyttöönotosta on saatavilla osoitteessa: www.eaton.com/greenmotionbuilding
Omaisuuden hallinta	Ohjelmisto- ja laitteisto-omaisuuden seuraaminen ympäristössäsi on edellytys kyberturvallisuuden tehokkaalle hallinnalle. Eaton suosittelee, että ylläpidät laiteluetteloa, jossa jokainen tärkeä komponentti yksilöidään yksiselitteisesti. Tämän helpottamiseksi **Eaton Green Motion Building** tukee seuraavia tunnistetietoja: Tuotteen tuotenumero, sarjanumero (löytyy tuotteesta), tehtaan hotspot-kirjautumistiedot ja asennetun ohjelmiston versio. Edellä mainitut tiedot löytyvät tyyppikilvestä ja konfigurointisivulta (lisätietoja on asennusohjeessa).
Riskinarviointi	Eaton suosittelee riskinarvioinnin suorittamista **Eaton Green Motion Buildingin** ja sen ympäristön luottamuksellisuuteen, saatavuuteen ja eheyteen kohdistuvien kohtuudella ennakoitavissa olevien sisäisten ja ulkoisten riskien tunnistamiseksi ja arvioimiseksi. Harjoitus olisi suoritettava sovellettavien teknisten ja sääntelypuitteiden, kuten IEC 62443:n ja NERC-CIP:n, mukaisesti. Riskinarviointi olisi toistettava määräajoin.
Fyysinen turvallisuus	Hyökkääjä, jolla on luvaton fyysinen pääsy, voi aiheuttaa vakavia häiriöitä järjestelmän/laitteen toiminnalle. Lisäksi teollisuuden ohjausprotokollat eivät tarjoa kryptografisia suojauksia, mikä tekee ICS- ja SCADA-viestinnästä erityisen haavoittuvaa niiden luottamuksellisuuteen kohdistuville uhkille. Fyysinen turvallisuus on tärkeä puolustuskeino tällaisissa tapauksissa.**Eaton Green Motion Building** on suunniteltu käyttöönotettavaksi ja käytettäväksi fyysisesti turvallisessa paikassa. Seuraavassa on joitakin parhaita käytäntöjä, joita Eaton suosittelee järjestelmän/laitteen fyysiseen suojaamiseen: • Varmistetaan tilat ja laitehuoneet tai -komerot kulunvalvontamekanismeilla, kuten lukoilla, kortinlukijoilla, vartijoilla, kameravalvonnalla jne. tarpeen mukaan. • Rajoita fyysistä pääsyä **Eaton Green Motion Buildingia** sisältäviin kaappeihin ja/tai koteloihin. EV-laturit on varustettu peukaloinnin estotoiminnolla. Kun laite avataan virta päällä -tilassa, ilmoitus lähetetään valvontaverkkoon. • Fyysistä pääsyä tietoliikennelinjoihin ja verkkokaapelointeihin olisi rajoitettava viestinnän kuuntelu- tai sabotaasiyrityksiltä suojautumiseksi. Laitekaappien välissä kulkeviin verkkokaapelointeihin on suositeltavaa käyttää metalliputkia. • **Eaton Green Motion Building** tukee seuraavia fyysisiä portteja: Sarjaportti (vain teknistä tukea varten), Ethernet-RJ45. Pääsyä näihin portteihin on rajoitettava. • Älä liitä irrotettavia tietovälineitä (esim. USB-laitteita, SD-kortteja jne.) mihinkään toimintoon (esim. laiteohjelmiston päivitys, kokoonpanon muuttaminen tai käynnistyssovelluksen muuttaminen), ellei tietovälineen alkuperä ole tiedossa ja luotettava. • Ennen kuin liität kannettavan laitteen USB-portin tai SD-korttipaikan kautta, tarkista laite haittaohjelmien ja virusten varalta.
Ajan synkronointi	Monet sähköverkkojen ja tietoverkkojen toiminnot riippuvat suuresti tarkasta aikatiedosta. Varmista, että järjestelmän kello on synkronoitu arvovaltaisen aikalähteen kanssa (manuaalisen määrityksen, NTP:n, SNTP:n tai IEEE 1588:n avulla). Ajan synkronointi tapahtuu automaattisesti, kun laite saa yhteyden OCPP Boot Notification- ja Heartbeat-järjestelmään, kun se on kytketty verkkoon.

Kategoria	Kuvaus
Verkon turvallisuus	**Eaton Green Motion Building** tukee verkkoviestintää ympäristön muiden laitteiden kanssa. Tämä ominaisuus voi aiheuttaa riskejä, jos sitä ei ole määritetty turvallisesti. Seuraavassa on Eatonin suosittelemia parhaita käytäntöjä verkon suojaamiseksi. Lisätietoja erilaisista verkon suojausstrategioista on saatavilla Eatonin julkaisussa Eaton kyberturvallisuutta koskevia näkökohtia sähkönjakelujärjestelmille [R1]. Eaton suosittelee verkkojen segmentointia loogisiin erillisalueisiin, segmenttien välisen liikenteen kieltämistä lukuun ottamatta erikseen sallittua liikennettä ja tiedonsiirron rajoittamista isännän ja isännän välisiin reitteihin (esimerkiksi reitittimen ACL-sääntöjen ja palomuurisääntöjen avulla). Tämä auttaa suojaamaan arkaluonteisia tietoja ja kriittisiä palveluita ja luo lisäesteitä, jos verkon rajoja rikotaan. Vähintäänkin yleishyödyllisen laitoksen teollisten ohjausjärjestelmien verkko olisi segmentoitava kolmiportaiseen arkkitehtuuriin (kuten NIST SP 800-82[R3]-julkaisussa suositellaan) paremman turvallisuusvalvonnan varmistamiseksi. Viestinnän suojaus: **Eaton Green Motion Building** salaa verkkoviestintänsä. Tämä salaus on aina oletusarvoisesti aktivoitu (HTTPS konfigurointisivulle, OCPP-turvaprofiili 2), eikä sitä tarvitse määrittää. Eaton suosittelee avaamaan vain ne portit, joita **toiminta edellyttää**, ja suojaamaan verkkoviestinnän verkon suojausjärjestelmillä, kuten palomuureilla ja tunkeutumisen havaitsemisjärjestelmillä / tunkeutumisen estojärjestelmillä.. Määritä palomuurisääntöjäsi alla olevien tietojen avulla, jotta **Eaton Green Motion Building** häiriötön toiminta on mahdollista. • TCP-portin 5355 on oltava auki LLMNR:n (TCP/UDP) mahdollistamiseksi • TCP-portin 443 on oltava auki, jotta OCPP-yhteys CPO-taustajärjestelmään on mahdollista 4G-modeemi, joka on kytketty sarja-USB:n kautta suorittimeen, käyttää point-to-point-protokollaa (ppp). On suositeltavaa käyttää **4G IoT SIM-kortteja**, jotka tukevat alla mainittuja tietoturvaominaisuuksia, jotta latausaseman ja palvelimen välinen internet-yhteys voidaan muodostaa. **Suositellut turvaominaisuudet** • Voit käyttää yksityistä APN-nimeä (Access Point Name), kun asennat Green Motion Buildingin ja otat latausverkon hallinnan käyttöön. • Käyttää 4G SIM-palveluntarjoajia, jotka tarjoavat mahdollisuuden salata tiedonsiirto joko virtuaalisen yksityisverkon (VPN) tai IPSec-suojauksen avulla, jotta voidaan ottaa käyttöön UICC-piiri (Universal integrated circuit card) -piikki, joka estää luvattoman pääsyn verkkoon. Modbus TCP:lle EV Charger tarjoaa IP whitelisting(valkoinen lista) -turvatoiminnon. On suositeltavaa, että käyttäjä lisää IP-osoitteen valkoiselle listalle. Lisätietoja tästä on asennusoppaan kohdassa Laitteen ja verkon konfigurointi.
Kirjaaminen ja tapahtumien hallinta	• Eaton suosittelee kaikkien asiaankuuluvien järjestelmä- ja sovellustapahtumien kirjaamista, mukaan lukien kaikki hallinto- ja ylläpitotoimet. • Lokit olisi suojattava peukaloinnilta ja muilta niiden eheyteen kohdistuvilta riskeiltä (esimerkiksi rajoittamalla lokien käyttö- ja muokkausoikeuksia, siirtämällä lokit turvallisuustietojen ja tapahtumien hallintajärjestelmään jne.) • Varmista, että lokit säilytetään kohtuullisen ja asianmukaisen ajan. • Tarkista lokit säännöllisesti. Tarkastustiheyden olisi oltava kohtuullinen ottaen huomioon järjestelmän, laitteen ja sen käsittelemien tietojen arkaluonteisuus ja kriittisyys. • Lokit ovat saatavilla Eaton Charging -verkonhallinnasta, lisätietoja on teknisessä dokumentaatiossa tai ottamalla yhteyttä paikalliseen tukitiimiin.
Haittaohjelmien suojaus	Eaton suosittelee riittävien haittaohjelmasuojausten käyttöönottoa tuotteen tai Eaton-tuotteen käyttämiseen käytettävien alustojen suojaamiseksi.

Kategoria	Kuvaus
Turvallinen ylläpito	Laitteessa on SSH-yhteys, jonka avulla huoltoteknikko voi suorittaa laitteen vianmäärityksen. SSH-portti on oletusarvoisesti poistettu käytöstä, ja sen huoltoteknikko saa ottaa käyttöön vain, jos se on ehdottoman välttämätöntä. **Parhaat käytännöt** Päivitä laitteen laiteohjelmisto ennen laitteen käyttöönottoa. Käytä sen jälkeen laiteohjelmistopäivityksiä ja ohjelmistokorjauksia säännöllisesti. Eaton julkaisee korjauksia ja päivityksiä tuotteisiinsa suojatakseen ne havaituilta haavoittuvuuksilta. Eaton kannustaa asiakkaita pitämään yllä johdonmukaista prosessia uusien laiteohjelmistopäivitysten seuraamiseksi ja asentamiseksi viipymättä. Laiteohjelmistopäivityksiä hallitaan ja asennetaan yksinomaan Eaton Charging Network Managerin kautta, mikä varmistaa, että käytät luotettavia laiteohjelmistotiedostoja. Offline-laitteissa on noudatettava seuraavaa menettelyä: 1. Avaa Konfiguraatio-verkkosivu 2. Valitse firmware GM-paketti ja paina upload 3. Laite lataa paketin ja tarkistaa allekirjoituksen 4. Laite lataa paketin ja tarkistaa allekirjoituksen Paikallista verkkopalvelinta voidaan käyttää myös laiteohjelmiston turvalliseen päivittämiseen.
Arkaluonteisten tietojen paljastaminen	Eaton suosittelee, että **Eaton Green Motion Building** mahdollisesti tallentamat arkaluonteiset tiedot (esim. yhteydet, lokitiedot, henkilötiedot) suojataan asianmukaisesti käyttämällä organisaation turvallisuuskäytäntöjä. Latauslaitteisiin tallennettuja mahdollisia arkaluonteisia tietoja ovat latausaseman viimeisen käyttäjän RFID-sarjatiedot.

Kategoria	Kuvaus
Käytöstä poistaminen tai nollaaminen	Paras käytäntö on puhdistaa tiedot ennen tietoja sisältävän laitteen hävittämistä. Käytöstäpoistoa koskevat ohjeet on esitetty asiakirjassa NIST SP 800-88. Eaton suosittelee, että sulautettua flash-muistia sisältävät tuotteet tuhotaan turvallisesti, jotta varmistetaan, ettei tietoja voida palauttaa.  **Sanitization and disposition decision flow** * Kuva ja tiedot NIST SP800-88:sta. Latausasema kierrätetään ISO9001-prosessin mukaisesti. **Sulautettu Flash-muisti piirilevyissä ja laitteissa** Eaton suosittelee seuraavia menetelmiä emolevyjen, oheiskorttien, kuten verkkosovittimien, tai muiden haihtumatonta flash-muistia sisältävien sovittimien hävittämiseksi. **Kirkas:** Palauta tila alkuperäisiin tehdasasetuksiin painamalla nollauspainiketta ja pitämällä sitä painettuna vähintään 5 sekunnin ajan. Katso lisätietoja teknisestä dokumentaatiosta. **Puhdistus:** Flash-muistia ei voi helposti tunnistaa ja irrottaa levystä. Tästä syystä Eaton suosittelee tuhoamaan koko laskentakortin. **Tuhoa:** Silppua, hajota, pulveroi tai polta laite polttamalla se luvan saaneessa polttolaitoksessa.

Viitteet

[R1] Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Cybersecurity Best Practices Checklist Reminder (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Guide to Industrial Control Systems (ICS) Security, May 2015:
https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

[R4] National Institute of Technology (NIST) Interagency "Guidelines on Firewalls and Firewall Policy, NIST Special Publication 800-41", October 2009:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Guidelines for Media Sanitization, September 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] Cybersecurity Best Practices for Modern Vehicles - NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] A Summary of Cybersecurity Best Practices - Homeland Security
https://www.hsdl.org/?view&did=806518

[R8] Characterization of Potential Security Threats in Modern Automobiles - NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Threat Modeling for Automotive Security Analysis
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

Eaton Industries Manufacturing GmbH
Place de la Gare 2
1345 Le Lieu, Sveitsi

Julkaisun nro MZ191002FI
Elokuu 2023

Seuraa meitä sosiaalisessa mediassa saadaksesi uusimmat tuote- ja tukitiedot.