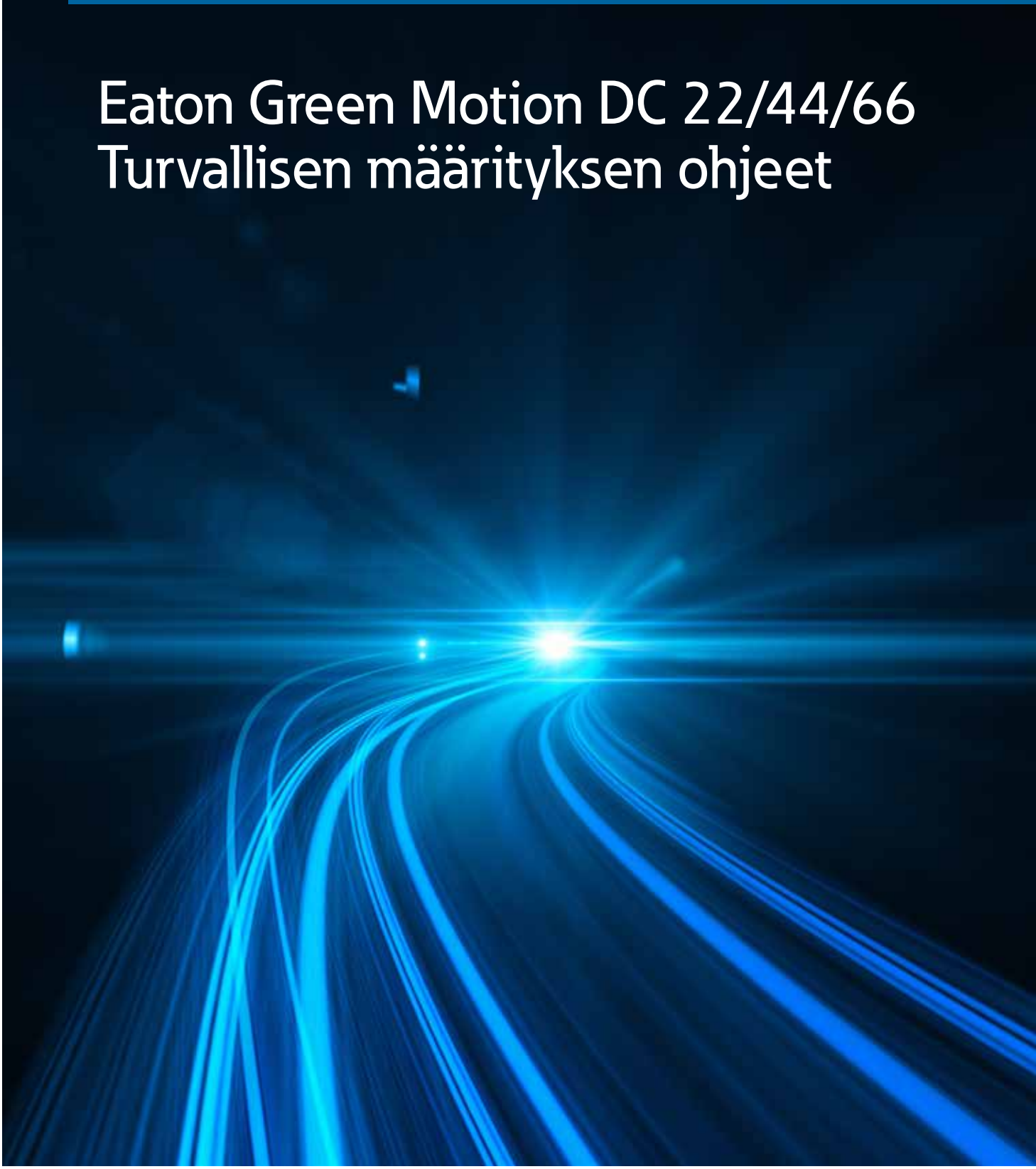
Eaton Cybersecurity Center of Excellence
Kyberturvallisuutta koskevat suositukset

Eaton Green Motion DC 22/44/66 Turvallisen määrityksen ohjeet



Powering Business Worldwide

Eaton-tuotteiden turvallista käyttöönottoa ja määritystä koskevat asiakirjat

Eaton Green Motion DC 22/44/66 -sähköauton latauslaitteet on suunniteltu kyberturvallisuutta silmällä pitäen. Tuotteessa on useita kyberturvallisuusriskien hallintaan liittyviä ominaisuuksia. Kyberturvallisuussuositukset sisältävät tietoja, joiden avulla käyttäjät voivat ottaa tuotteen käyttöön ja ylläpitää sitä tavalla, joka minimoi kyberturvallisuusriskit. Näiden kyberturvallisuussuositusten ei ole tarkoitus antaa kattavaa opasta kyberturvallisuuteen, vaan täydentää asiakkaan olemassa olevia kyberturvallisuusohjelmia.

Eaton on sitoutunut minimoimaan tuotteidensa kyberturvallisuusriskit ja käyttämään kyberturvallisuuden parhaita käytäntöjä tuotteissaan ja ratkaisuissaan, jotta ne olisivat turvallisempia, luotettavampia ja kilpailukykyisempiä asiakkaille.

Seuraavissa raporteissa on lisätietoja kyberturvallisuuden parhaista käytännöistä ja ohjeista:

Kyberturvallisuushuomiot sähkönjakelujärjestelmille (WP152002EN):

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

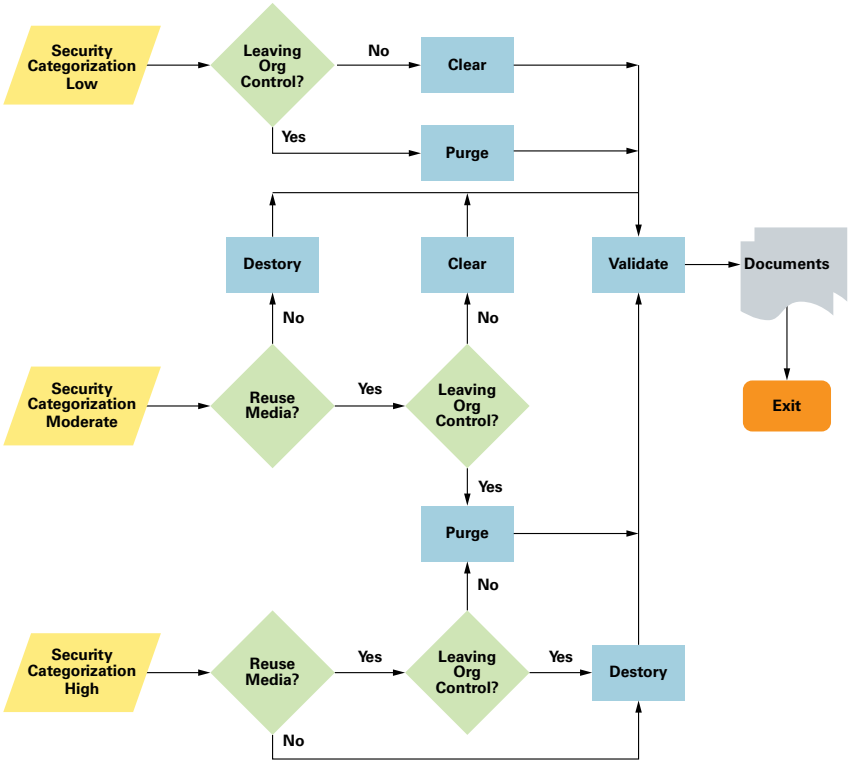
Kyberturvallisuuden parhaiden käytäntöjen tarkistuslista (WP910003EN):

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

Kategoria	Kuvaus
Käyttötarkoitus ja käyttöönotto	Otetaan käyttöön asiakkaan alueella yksityisissä tai julkisissa pysäköintitiloissa, esimerkiksi sähköautojen lataamista, todentamista ja laskutusta varten. Julkisiin tiloihin asennettujen laturien käyttäjät todennetaan yksilöllisesti RFID-korttien avulla. Loppukäyttäjä voi käyttää HMI:tä esimerkiksi lataustyyppiä, pistokkeen tyyppiä ja käyttötilastoja koskevien tietojen määrittämiseen/hakemiseen. Lisätietoja on tuotteen käyttöoppaassa.
Resurssien hallinta	Kyberturvallisuuden tehokas hallinta edellyttää ohjelmistojen ja laitteistojen seurantaa ympäristössäsi. Eaton suosittelee, että ylläpidät resurssivarastoa, joka tunnistaa yksilöllisesti jokaisen tärkeän komponentin. Tämän helpottamiseksi **Eaton Green Motion DC 22/44/66** tukee seuraavia tunnistetietoja: Tuoteluettelon numero, sarjanumero (saatavilla tuotteessa). Lisätietoja on asennusoppaassa.
Riskien arviointi	Eaton suosittelee riskien arviointia **Eaton Green Motion DC 22/44/66** -sähköautolaturin ja sen ympäristön luottamuksellisuuden, käytettävyyden ja eheyden kohtuullisesti ennakoitavien sisäisten ja ulkoisten riskien tunnistamiseen ja arviointiin. Tämä tulee suorittaa soveltuvien teknisten ja lainsäädännöllisten periaatteiden, kuten IEC 62443 ja NERC-CIP, mukaisesti. Riskien arviointi on toistettava säännöllisesti.
Fyysinen suojaus	Luvaton fyysinen pääsy voi aiheuttaa vakavia häiriöitä järjestelmän/laitteen toimintaan. Fyysinen suojaus on tällaisissa tapauksissa tärkeä puolustuskeino. **Eaton Green Motion DC 22/44/66** on suunniteltu käytettäväksi fyysisesti suojatussa paikassa. Eaton suosittelee seuraavia käytäntöjä järjestelmän/laitteen fyysiseen suojaamiseen: • Varusta tilat ja laitehuoneet tai -kaapit tarvittaessa kulunvalvontamekanismeilla, kuten lukoilla, pääsykortinlukijoilla, henkilösuluilla ja kameravalvontajärjestelmillä, tai järjestä vartiointi. • Fyysistä pääsyä tiedonsiirto- ja verkkokaapeleille on rajoitettava, jotta voidaan suojautua tiedonsiirron katkaisu- ja sabotaasiyrityksiltä. On suositeltavaa käyttää laitekaappien välisten verkkokaapeleiden johdotukseen metallisia asennusputkia. • **Eaton Green Motion DC 22/44/66** tukee seuraavia fyysisiä portteja: Ethernet, sarjaportti ja USB-portti. Näiden porttien luvaton käyttö on estettävä. • Älä liitä siirrettäviä tallennusvälineitä (esimerkiksi USB-laitteita tai SD-kortteja).
Tilien hallinta	Järjestelmän looginen käyttö: Laitetta saavat käyttää vain sallitut käyttäjät. Joitakin seuraavista käytännöistä on ehkä otettava käyttöön, ja henkilöille on määritettävä vain ne oikeudet, jotka ovat välttämättömiä heidän työroolinsa/toimintojensa toteuttamisen kannalta. Joitakin seuraavista käytännöistä on ehkä otettava käyttöön: - Varmista, että oletustunnistetiedot vaihdetaan ensimmäisen kirjautumisen yhteydessä. Niitä ei tule käyttää tuotantoympäristöissä, koska oletustunnistetiedot ovat yleisesti tiedossa. - Ei tilien jakamista – jokaiselle käyttäjälle on määritettävä yksilöllinen tili yhteisten tilien ja salasanojen sijaan. Tuotteen valvonta- ja kirjautumistoiminnot on suunniteltu sen pohjalta, että jokaisella käyttäjällä on yksilöllinen tili. Tunnistetietojen jakaminen heikentää turvallisuutta. - Varmista, että salasanan pituus, monimutkaisuus ja vanhenemisvaatimukset on määritetty oikein, erityisesti kaikille hallinnollisille tileille (esimerkiksi vähintään 10 merkkiä, sekoitus isoja ja pieniä kirjaimia sekä erikoismerkkejä, vanhenevat 90 päivän välein tai muutoin organisaation käytäntöjen mukaisesti. Sarja- ja SSH-tilit on tarkoitettu vain Eatonin teknisen tuen käyttöön vianetsintää ja -määritystä varten.
Ajan synkronointi	Monet sähköverkkojen ja IT-verkkojen toiminnot ovat riippuvaisia tarkoista ajoitustiedoista. Varmista, että järjestelmän kello on synkronoitu määräävän aikalähteen kanssa (manuaalinen määritys NTP, SNTP tai IEEE 1588). Ajan synkronointi tapahtuu automaattisesti, kun laite on yhdistetty verkkoon ja se voi käyttää OCPP-käynnistys- ja täsmäytystoimintoja. Kaikissa aikaleimoissa käytetään UTC-aikavyöhykettä referenssinä.
Tietoverkkoturvallisuus	Eaton Green Motion DC 22/44/66 tukee tiedonsiirtoa muiden ympäristön laitteiden kanssa. Tämä ominaisuus voi aiheuttaa riskejä, jos sitä ei ole määritetty oikein. Seuraavat ovat Eatonin suosittelemia käytäntöjä verkon turvaamiseksi. Lisätietoja tietoverkon suojausstrategioista on Eatonin raportissa Kyberturvallisuushuomiot sähkönjakelujärjestelmille [R1]. Eaton suosittelee tietoverkkojen segmentointia loogisiksi alueiksi, segmenttien välisen liikenteen estämistä erikseen sallittuja lukuun ottamatta sekä tiedonsiirron rajoittamista isäntäkoneiden välisiin polkuihin (esimerkiksi reitittimen ACL:n ja palomuurisääntöjen avulla). Tämä auttaa suojaamaan arkaluontoisia tietoja ja kriittisiä palveluja ja tuo lisäturvaa verkkomurtotilanteissa. Teollisuuden ohjausjärjestelmien verkko on jaoteltava vähintään kolmikerroksiseen arkkitehtuuriin (NIST SP 800-82[R3]:n suositusten mukaisesti) turvallisuuden parantamiseksi.

Kategoria	Kuvaus
	Tiedonsiirron suojaus: Eaton Green Motion DC 22/44/66 salaa verkkoyhteytensä. Tämä salaus on oletusarvoisesti käytössä. Eaton suosittelee ottamaan käyttöön vain ne portit, joita toiminnoissa tarvitaan, ja suojaamaan verkkoviestintää käyttämällä verkon suojausjärjestelmiä, kuten palomuureja ja tunkeutumisen havaitsemisjärjestelmiä / tunkeutumisen estojärjestelmiä. Online-tilassa laturi muodostaa yhteyden taustajärjestelmään käyttämällä OCPP-protokollaa 4G-yhteyden tai Ethernet-yhteyden kautta. On suositeltavaa käyttää Eatonin toimittamaa SIM-korttia. Jos asiakas haluaa hankkia oman SIM-korttinsa, on suositeltavaa käyttää 4G IoT -SIM-kortteja teleoperaattorilta, joka tukee seuraavia suositeltuja tietoturvaominaisuuksia. Suositellut tietoturvaominaisuudet Käytä SIM-korttia, joka tarjoaa yksityisen tukiaseman nimen (APN) xChargeln Mobility -asennuksen ja Charging Network Managerin käyttöönoton aikana. Julkista APN:ää käyttäviä SIM-kortteja ei ole suositeltavaa käyttää, koska ne eivät suojaa kyberturvallisuusriskeiltä. Valitse 4G SIM -palveluntarjoaja, joka tarjoaa mahdollisuuden salata tiedonsiirto joko VPN (Virtual Private Network) -verkon tai IPSec-suojauksen avulla 4G-tiedonsiirrossa. Käytä SIM-korttia, jonka avulla voit ottaa käyttöön UICC (Universal Integrated Circuit Card) -piirikortin PIN-koodin, jolla voi estää verkon luvattoman käytön. Käytä SIM-korttia, joka suojaa varkauksilta ja SIM-kloonaukselta. Älä käytä julkista APN:ää käyttäviä vapaasti saatavilla olevia SIM-kortteja, sillä niitä ei ole tarkoitettu kaupallisille IoT-tuotteille. **Note:** Julkista APN:ää käyttäviä SIM-kortteja ei ole suositeltavaa käyttää, koska ne eivät suojaa kyberturvallisuusriskeiltä.
Etäkäyttö	Laitteiden/järjestelmien etäkäyttö luo verkkoon uuden pääsyreitin. Tällaisen pääsyreitin tiukka hallinta ja vahvistaminen on olennaisen tärkeää ICS-tietoturvan ylläpidon kannalta. • Etäkäyttötoiminnot mahdollistaa suojausprotokolla OCPP TLS 1.2:n yli. • Laite lähettää järjestelmälokeissa kirjatut toiminnot taustajärjestelmään OCPP-protokollan kautta. • Laiteohjelmistopäivitykset siirretään laitteisiin taustajärjestelmästä OCPP:n kautta, jos laite on yhteydessä verkkoon. • Lisätietoja on saatavissa Eatonin kyberturvallisuuden parhaissa käytännöissä [R2].
Kirjaaminen ja tapahtumien hallinta	Lokeja on saatavilla Eaton Charging Network Managerissa (taustajärjestelmä). Lisätietoja saat tuotteen teknisestä dokumentaatiosta tai paikalliselta tukitiimiltä.
Haittaohjelmilta suojautuminen	Eaton suosittelee, että tuote tai Eaton-tuotteessa käytettävät alustat suojataan asianmukaisesti haittaohjelmilta.
Turvallinen ylläpito	Laite sisältää paikallisen SSH-yhteyden, jonka avulla huoltoinsinööri voi suorittaa laitteen toimintojen vianmäärityksen järjestelmänvalvojan avulla. SSH-portti on oletusarvoisesti poissa käytöstä. Tämä liitäntä on tarkoitettu vain huoltoinsinööreille. Asiakkaan ei pidä käyttää tätä toimintoa. **Note:** TCP-portti 22 on tarkoitettu vain diagnostiseen käyttöön, eikä sitä saa jättää käyttöön. **Parhaat käytännöt** Päivitä laiteohjelmisto ennen laitteen käyttöönottoa tuotannossa. Asenna sen jälkeen laiteohjelmistopäivitykset ja ohjelmistopäivitykset säännöllisesti. Eaton julkaisee tuotteisiinsa korjauksia ja päivityksiä, jotka suojaavat niitä havaituilta haavoittuvuuksilta. Laiteohjelmistopäivityksiä hallitaan ja asennetaan Eatonin Charging Network Manager -ohjelmiston kautta, mikä varmistaa, että käytät luotettavia laiteohjelmistotiedostoja. Tai tunnettujen kolmansien osapuolten CNM:n kautta (joka saa luotettavat laiteohjelmistotiedostot Eatonilta). • Jos sähköauton latauslaite on online-tilassa (yhteydessä Internetiin), se päivittyy automaattisesti, kun päivitys on saatavilla. Sähköautolaturi ei ole käytettävissä, kun laite päivittää laiteohjelmistoa.

Kategoria	Kuvaus
Käytöstä poistaminen tai nollaus	On suositeltavaa tyhjentää tiedot ennen minkään tietoja sisältävän laitteen hävittämistä. Käytöstä poiston ohjeet ovat NIST SP 800-88:ssa. Eaton suosittelee, että sisäisen Flash-muistin sisältävät tuotteet tuhotaan tietoturvakäytäntöjen mukaisesti, jotta tietoja ei voida palauttaa. Flash-muistin voi tyhjentää tehdasasetusten palautustoiminnolla. Lisätietoja on asennusoppaassa.



Sanitization and disposition decision flow

* Kuva ja tiedot NIST SP800-88:sta

Latausasema kierrätetään prosessin ISO9001 mukaisesti.

Sisäinen Flash-muisti piirikorteissa ja laitteissa

Eaton suosittelee seuraavia menetelmiä emolevyjen ja lisäkorttien, kuten verkkosovittimien tai minkä tahansa muun pysyvää muistia sisältävän sovittimen, hävittämiseen.

Tyhjennys: Palauta tehdasasetukset painamalla nollauspainiketta vähintään 5 sekunnin ajan. Katso lisätietoja teknisestä dokumentaatiosta.

Poisto: Flash-muistia ei voi tunnistaa ja irrottaa kortista helposti. Tästä syystä Eaton suosittelee tuhoamaan koko kortin.

Tuhoaminen: Silppua, hajota tai murskaa laite tai polta se hyväksytyssä jätteenpolttouunissa.

Lähteet

[R1] Kyberturvallisuushuomiot sähkönjakelujärjestelmille (WP152002EN):
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

[R2] Kyberturvallisuuden parhaiden käytäntöjen tarkistuslista (WP910003EN):
https://www.eaton.com/content/dam/eaton/company/news-insights/cybersecurity/white-papers/WP910003EN.pdf

[R3] NIST SP 800-82 Rev 2, Opas teollisuuden ohjausjärjestelmien (ICS) tietoturvaan, toukokuu 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", lokakuu 2009:
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

[R5] NIST SP 800-88, Ohjeet datan poistamiseen, syyskuu 2006:
http://ws680.nist.gov/publication/get_pdf.cfm?pub_id=50819

[R6] Nykyaikaisten ajoneuvojen kyberturvallisuuden parhaat käytännöt – NHTSA
https://www.nhtsa.gov/staticfiles/nvs/pdf/812333_CybersecurityForModernVehicles.pdf

[R7] Yhteenveto kyberturvallisuuden parhaista käytännöistä – Yhdysvaltojen sisäisen turvallisuuden ministeriö
https://www.hsdl.org/?view&did=806518

[R8] Nykyaikaisten autojen mahdollisten tietoturvauhkien luonnehdinta – NHTSA
https://www.nhtsa.gov/DOT/NHTSA/NVS/Crash%20Avoidance/Technical%20Publications/2014/812074_Characterization_PotentialThreatsAutos(1).pdf

[R9] Uhkien mallinnus autoteollisuuden tietoturva-analyysia varten
http://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-41r1.pdf

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

Julkaisunumero MZ192001FI
Lokakuu 2023

Seuraa meitä sosiaalisessa mediassa, ja saat tuoreimmat tuote- ja tukitiedot.

Powering Business Worldwide