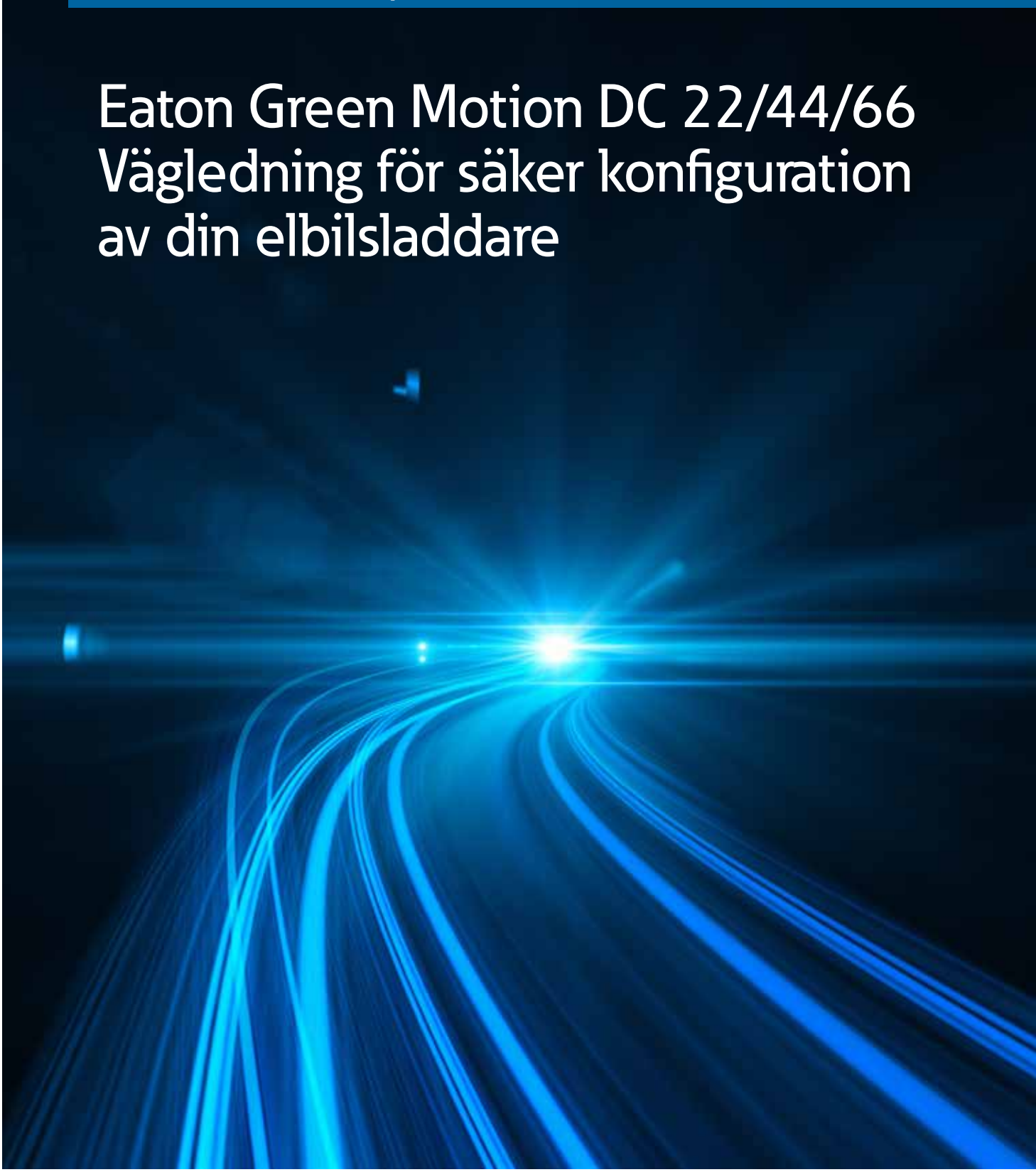
Eaton Cybersecurity Center of Excellence
Rekommendationer för cybersäkerhet

Eaton Green Motion DC 22/44/66 Vägledning för säker konfiguration av din elbilsladdare



Powering Business Worldwide

Dokumentation om hur man på ett säkert sätt installerar och konfigurerar Eatons produkter

Elbilsladdarna Eaton Green Motion DC 22/44/66 har utvecklats med cybersäkerhet i åtanke. Ett flertal funktioner ingår i produkten för att hantera riskerna kring cybersäkerhet. Dessa rekommendationer för cybersäkerhet innehåller information som hjälper användare att driftsätta och underhålla produkten på ett sätt som minimerar riskerna kring cybersäkerhet. Dessa rekommendationer för cybersäkerhet är inte avsedda att fungera som en heltäckande vägledning för cybersäkerhet, utan snarare som ett komplement till kundernas befintliga cybersäkerhetsprogram.

Eaton har åtagit sig att minimera riskerna kring cybersäkerhet för sina produkter samt implementera bästa möjliga praxis för cybersäkerhet i sina produkter och lösningar, vilket gör dem säkrare, mer tillförlitliga och konkurrenskraftiga för kunderna.

I följande rapporter finns mer information om allmänna rekommendationer och riktlinjer för cybersäkerhet:

Cybersecurity Considerations for Electrical Distribution Systems (WP152002EN):

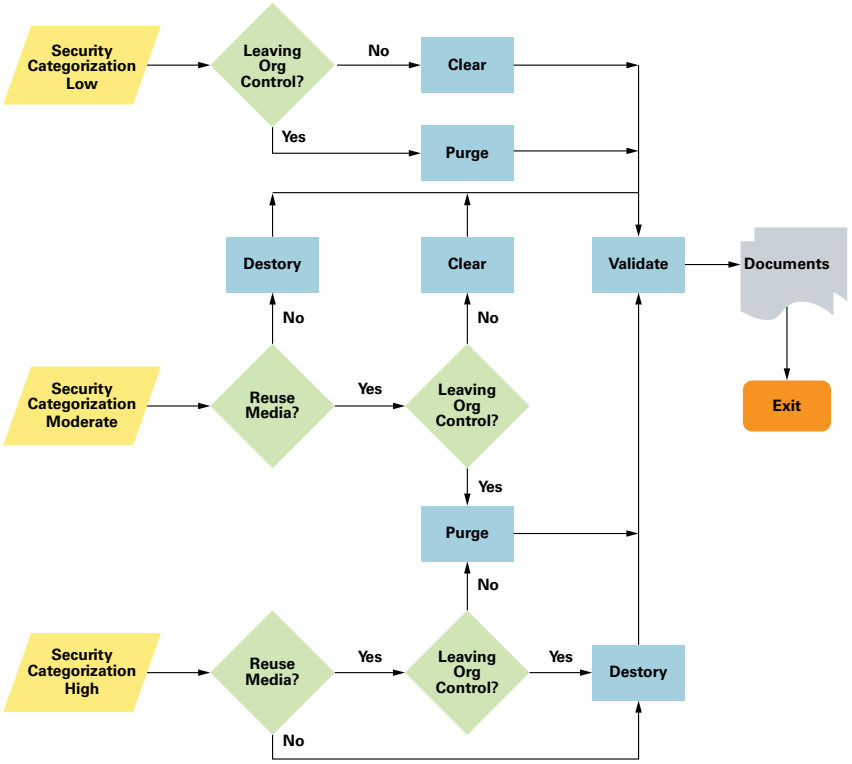
http://www.eaton.com/ecm/groups/public/@pub/@eaton/@corp/documents/content/pct_1603172.pdf

Cybersecurity Best Practices Checklist Reminder (WP910003EN):

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

Kategori	Beskrivning
Avsedd användning och driftsättningskontext	Driftsätts hos kunden på privata och allmänna parkeringsplatser för att möjliggöra laddning av elfordon, autentisering, fakturering osv. För laddare som monteras på offentliga platser använder användarna RFID-kort för unik identifiering. Slutanvändaren kan använda HMI för att ange/erhålla information som rör typen av laddning, typen av kontakt, användningsstatistik osv. Se produktens bruksanvisning för ytterligare information.
Tillgångsöversikt	Att hålla reda på program- och hårdvarutillgångar i din omgivning är en förutsättning för att kunna hantera cybersäkerhet på ett effektivt sätt. Eaton rekommenderar att du upprätthåller en tillgångsinventering som unikt identifierar varje viktig komponent. För att underlätta detta stöder **Eaton Green Motion DC 22/44/66** följande identifieringsinformation: Produktkatalognummer, serienummer, (finns på produkten). Se installationsanvisningarna för mer information.
Riskbedömning	Eaton rekommenderar att en riskbedömning genomförs för att identifiera och bedöma rimligt förutsebara interna och externa risker för sekretessen, tillgängligheten och integriteten hos **Eaton Green Motion DC 22/44/66** och dess omgivning. Denna process bör genomföras i enlighet med tillämpliga tekniska och rättsliga regelverk, t.ex. IEC 62443 och NERC-CIP. Riskbedömningen bör upprepas med jämna mellanrum.
Fysisk säkerhet	En angripare med obehörigt fysiskt tillträde kan orsaka allvarliga störningar i systemets/enhetens funktioner. Fysisk säkerhet är en viktig del av försvaret i sådana fall. **Eaton Green Motion DC 22/44/66** är utformad för att monteras och driftsättas på en fysiskt säker plats. Nedan följer några av de bästa åtgärderna som Eaton rekommenderar för att fysiskt säkra ditt system/din enhet: • Säkra anläggningen och utrustningsrum eller förråd med säkerhetsutrustning för tillträde såsom lås, kortläsare, vakter, slussdörrar, övervakningskameror osv. efter behov. • Fysiskt tillträde till telekommunikationslinjer och nätverkskablar bör begränsas för att skydda mot försök att avlyssna eller sabotera kommunikation. Det är rekommenderat att använda metallrör för nätverkskablar som löper mellan apparatskåp. • **Eaton Green Motion DC 22/44/66** har stöd för följande portar för fysisk åtkomst: Ethernet, seriell port, USB-port. Åtkomsten till dessa portar bör begränsas för ej auktoriserade användare. • Anslut inte flyttbara medier (t.ex. USB-enheter, SD-kort osv.).
Kontohantering	Logisk åtkomst till systemet: Enheten bör begränsas till legitima användare. Vissa av de följande rekommenderade rutinerna kan behöva implementeras och personer bör enbart tilldelas de behörigheter som krävs för att de ska kunna utföra sina arbetsuppgifter. Vissa av de följande rekommenderade rutinerna kan behöva implementeras: – Åtgärden med att ändra standardinloggningsuppgifterna vid första inloggningen bör inte genomföras i produktionsmiljöer med standarduppgifter eftersom de är allmänt kända. – Ingen kontodelning – samtliga användare ska tilldelas ett unikt konto istället för att dela konton och lösenord. Säkerhetsfunktionerna för övervakning och loggning i produkten har utformats baserat på att samtliga användare har ett unikt konto. Att ge användare möjlighet att dela inloggningsuppgifter påverkar säkerheten negativt. – Se till att kraven på lösenordens längd, komplexitet och giltighetsperiod är lämpliga, i synnerhet för alla administrativa konton (t.ex. minst tio tecken, blandning av stora och små bokstäver och specialtecken och en giltighetsperiod på 90 dagar, eller andra krav i enlighet med din organisations policyer). Serie- och SSH-konton är endast avsedda att användas av Eatons tekniska support för felsökning/felsökningssyfte.
Tidssynkronisering	Många funktioner i elnät och IT-nät är starkt beroende av exakt tidsinformation. Se till att systemklockan är synkroniserad med en tillförlitlig tidskälla (med manuell konfiguration, NTP, SNTP eller IEEE 1588). Tidssynkroniseringen sker automatiskt när enheten får tillgång till en OCPP-startavisering eller en pulsfrekvens när den är ansluten online. Alla tidsstämplar använder UTC-tidszonen som referens.
Nätverkssäkerhet	**Eaton Green Motion DC 22/44/66** stödjer nätverkskommunikation med andra enheter i omgivningen. Denna funktion kan medföra risker om den inte konfigureras på ett säkert sätt. Följande är Eatons rekommenderade praxis för att säkra nätverket. Ytterligare information om olika strategier för nätverkssäkerhet finns i Eaton Cybersecurity Considerations for Electrical Distribution Systems [R1]. Eaton rekommenderar att man segmenterar nätverk i logiska grupper, förhindrar trafik mellan segment om det inte uttryckligen tillåts, och begränsar kommunikationen till direkta vägar mellan värdar (t.ex. med hjälp av ACL:er och brandväggsregler). Detta bidrar till att skydda känslig information och kritiska tjänster och skapar ytterligare hinder i händelse av intrång i nätverkets perimeter. Som ett minimum bör ett industriellt styrsystem vara segmenterat i en arkitektur med tre lager (enligt rekommendationerna i NIST SP 800-82[R3]) för bättre säkerhetskontroll.

Kategori	Beskrivning
	Kommunikationsskydd: **Eaton Green Motion DC 22/44/66** erbjuder kryptering av nätverkskommunikation. Denna kryptering är alltid aktiverad som standard. Eaton rekommenderar att endast de portar som krävs för driften öppnas och att nätverkskommunikationen skyddas med hjälp av nätverksskydd såsom brandväggar och system för intrångsdetektering/system för intrångsskydd. I onlineläge ansluter laddaren till backend med hjälp av OCPP-protokoll via 4G-anslutning eller Ethernet. Vi rekommenderar att du använder det SIM-kort som Eaton tillhandahåller. Om kunden väljer att anskaffa sitt eget SIM-kort rekommenderar vi IoT-SIM-kort med 4G från en telekomtjänstleverantör med stöd för nedanstående rekommenderade säkerhetsfunktioner. Rekommenderade säkerhetsfunktioner Använd ett Access Point Name (APN) vid installation av Green Motion DC 22/44/66 och drifttagning av Charging Network Manager. Vi rekommenderar starkt att du inte använder SIM-kort med offentliga Access Point Name, eftersom de inte anses säkra vid cybersäkerhetsrisker. Använd 4G SIM-tjänsteleverantörer som tillhandahåller ett alternativ för att kryptera datakommunikation med antingen ett virtuellt privat nätverk (VPN) eller IPSec-skydd för 4G-kommunikation. Använd ett SIM-kort med en funktion som möjliggör aktivering av en PIN-kod till ett universellt integrerat kretskort (UICC) för att förhindra obehörig åtkomst till nätverket. Använd ett SIM-kort som erbjuder säkerhetsåtgärder mot stöld och kloning av SIM-kort. Använd inte SIM-kort tillgängliga över disk med offentliga Access Point Name, eftersom de inte är avsedda för kommersiella IoT-produkter. **Note:** Vi rekommenderar starkt att du inte använder SIM-kort med offentliga Access Point Name, eftersom de inte anses säkra vid cybersäkerhetsrisker.
Fjärråtkomst	Fjärråtkomst till enheter/system skapar ytterligare en ingångspunkt i nätverket. Strikt hantering och validering av upphörande av denna åtkomst är avgörande för att upprätthålla kontrollen över den övergripande ICS-säkerheten. • Fjärråtkomstfunktionerna erbjuds genom det säkra protokollet OCPP över TLS 1.2. • Enheten registrerar de aktiviteter som loggas under systemloggarna till det interna nätverket via OCPP-protokollet. • Uppdateringar av inbyggd programvara distribueras till enheterna från det interna nätverket via OCPP om enheterna är anslutna online. • För mer information ska du läsa Eatons bästa praxis för cybersäkerhet [R2]
Loggning och händelsehantering	Loggar finns tillgängliga från Eaton Charging Network Manager (internt nätverk). För ytterligare information ska du läsa den tekniska dokumentationen eller kontakta ditt lokala supportteam.
Försvar mot skadlig programvara	Eaton rekommenderar att lämpliga skydd mot skadlig programvara installeras för att skydda produkten eller de plattformar som används för att använda Eaton-produkten.
Säkert underhåll	Enheten har en lokal SSH-anslutning, så att en servicetekniker kan felsöka enhetens funktionalitet. SSH-porten är inaktiverad som standard. Denna anslutning är enbart avsedd för servicetekniker. Det är inte meningen att kunden ska använda denna funktion. **Note:** TCP-port 22 tillhandahålls i diagnostiksyfte och ska inte förbli aktiverad. **Bästa metod** Uppdatera enhetens inbyggda programvara innan den sätts i drift. Uppdatera därefter den inbyggda programvaran och korrigeringsfiler regelbundet. Eaton publicerar korrigeringsfiler och uppdateringar för sina produkter i syfte att skydda dem mot eventuella brister som upptäcks. Uppdateringar av inbyggd programvara ska hanteras och installeras via Eaton Charging Network Manager, vilket säkerställer att du använder betrodda filer för inbyggd programvara, eller via kända tredjeparters Charging Network Manager (de får betrodda filer för inbyggd programvara från Eaton). • För laddare i onlineläge (anslutna till internet) uppdateras elbilsladdaren automatiskt när en uppdatering är tillgänglig. Elbilsladdaren kommer inte att vara tillgänglig för laddning medan enheten uppgraderar den inbyggda programvaran.

Kategori	Beskrivning
Avveckling eller nollställning	Bästa praxis är att ta bort data innan en enhet som innehåller data kasseras. Riktlinjer för avveckling finns i NIST SP 800-88. Eaton rekommenderar att produkter som innehåller inbyggt flashminne förstörs på ett säkert sätt för att säkerställa att data inte kan återställas. Flashminnet kan raderas med hjälp av funktionen för fabriksåterställning. Se installationsanvisningarna för mer information.  **Sanitization and disposition decision flow** * Bild och data från NIST SP800-88 Laddningsstationen återvinns enligt process ISO9001. **Inbyggt flashminne på kort och enheter** Eaton rekommenderar följande metoder för kassering av moderkort, periferikort som nätverksadaptrar eller andra adaptrar som innehåller icke-flyktigt flashminne. **Rensa:** Återställ till de ursprungliga fabriksinställningarna genom att trycka på återställningsknappen och hålla den intryckt i minst 5 sekunder. Mer information finns i den tekniska dokumentationen. **Ta bort:** Flashminnet kan inte enkelt identifieras och tas bort från kortet. Av denna anledning rekommenderar Eaton att hela datorkortet förstörs. **Förstör:** Strimla, sönderdela, pulverisera eller förbränn enheten genom att bränna den i en godkänd förbränningsanläggning.

Referenser

[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, Schweiz
Eaton.com

Publikationsnr. MZ192001SV
Oktober 2023

Följ oss på sociala medier för att få den senaste produkt- och supportinformationen.