



Risicanalys av IoT-enhet med EN 18031

**En praktisk fallstudie av säkerhetsbrister och förbättringsåtgärder i en
uppkopplad EV-laddare**

Shakir Al Chsein

EXAMENSARBETE

Nätverksteknik med IT-säkerhetsprogrammet, 120hp

Sammanfattning

Detta arbete undersöker hur den europeiska standarden EN 18031 kan användas som ett strukturerat ramverk för riskanalys av IoT-enheter. Bakgrunden till arbetet är att IoT-enheter återkommande uppvisar säkerhetsbrister och att tillverkare behöver konkreta verktyg för att arbeta systematiskt med cybersäkerhet.

Arbetet genomfördes som kvalitativ fallstudie i samarbete med företaget iThing AB, där en verklig EV-laddare analyserades med EN 18031 som ramverk. Analysen följde standardens moduluppbyggnad och bedömde om enheten uppfyller varje krav baserat på teknisk dokumentation och information från iThing AB. Totalt analyserades 48 krav fördelade på standardens tre delar. Av dessa bedömdes 9 krav som Pass, 11 som Fail och 19 som Non-Conformity.

Resultaten visar att enheten uppfyller grundläggande krav inom autentisering, lösenordsunikhet och intern logglagring. Flera kritiska krav inom kommunikationsskydd, lagringssäkerhet och uppdateringsmekanismer uppfylls dock inte fullt ut. Förbättringsförslag togs fram inom samtliga identifierade bristområden.

Den viktigaste slutsatsen är att EN 18031 fungerar som ett praktiskt och användbart verktyg för riskanalys av IoT-enheter. En EN 18031-baserad analys kan hjälpa tillverkare att systematiskt identifiera och åtgärda säkerhetsbrister och utgör ett konkret förberedelsesteg inför Cyber Resilience Acts ikraftträdande.

Datum: 2026-03-19

Författare: Shakir Al Chsein

Examinator: Fatiha Djebbar

Handledare: Hani Alid (Högskolan Väst) och Conny Broberg (iThing AB)

Program: Nätverksteknik med IT-säkerhet, 120hp

Huvudområde: Datateknik

Utbildningsnivå: Grundnivå

Kurskod: EXN300, 7,5hp

Nyckelord: Riskanalys, IoT-säkerhet, EN 18031, elbilsladdare, cybersäkerhet, sårbarhetsanalys

Utgivare: Högskolan Väst, institutionen för ingenjörsvetenskap. 461 86 Trollhättan. Tel: 0520-22 30 00 Fax: 0520-22 32 99, www.hv.se

Summary

This thesis investigates how the European standard EN 18031 can be used as a structured framework for risk analysis of IoT devices. The background is that IoT devices frequently exhibit security vulnerabilities, and that manufacturers need concrete tools to work systematically with cybersecurity.

The work was conducted as a qualitative case study in collaboration with the company iThing AB, where a real EV charger was analyzed using EN 18031 as a framework. The analysis followed the standard modular structure and assessed whether the device meets each requirement based on technical documentation and information provided by the manufacturer. A total of 48 requirements were assessed across the three parts of the standard. Of these, 9 were assessed as Pass, 11 as Fail, and 19 as Non-Conformity.

The results show that the device meets basic requirements regarding authentication, password uniqueness, and internal log storage. However, several critical requirements related to communication security, storage protection, and update mechanisms were not fully met. Improvement recommendations were developed for all identified deficiency areas.

The most important conclusion is that EN 18031 functions as a practical and useful tool for risk analysis of IoT devices. An EN 18031-based analysis can help manufacturers systematically identify and address security vulnerabilities, and constitutes a concrete preparatory step ahead of the Cyber Resilience Act entering into force.

Ordlista

- EN 18031 – Europeisk standard som tillhandahåller ett strukturerat ramverk med säkerhetskrav för uppkopplade produkter, uppdelat i tre delar beroende på produktens funktion
- Cyber Resilience Act (CRA) - EU-förordning som från 2027 ställer bindande cybersäkerhetskrav på tillverkare av produkter med digitala element som säljs inom EU.
- OCPP (Open Charge Point Protocol) - Ett öppet kommunikationsprotokoll som används för datautbyte mellan EV-laddare och centrala hanteringssystem i molnet
- MQTT (Message Queuing Telemetry Transport) - Ett lättviktigt meddelandeprotokoll utformat för kommunikation mellan uppkopplade enheter med begränsad bandbredd eller processorkraft
- OTA (Over-the-Air) - En metod för att distribuera och installera programuppdateringar till en enhet trådlöst via internet, utan fysisk åtkomst till enheten.
- NVS-Flash - Ett icke-flyktigt lagringsutrymme i ESP32-mikrokontrollen där känsliga data som autentiseringsuppgifter och konfigurationsinställningar lagras persistent.
- Air Link - Den trådlösa kommunikationslänken mellan EV-laddaren och externa tjänster via WiFi, vilket utgör enhetens primära nätverksgränssnitt.

Table of Contents

1. Inledning	7
1.1 Kontext och motivering	7
1.2 Problemformulering	7
1.3 Syfte och frågeställningar	7
1.4 Avgränsning	8
1.5 Disposition	8
2. Bakgrund	8
2.1 IoT-säkerhet	8
2.2 EN 18031	9
2.3 Cyber Resilience Act	10
2.4 TARA och ISO/SAE 21434	11
2.5 Relaterat arbete	11
3. Metod	13
3.1 Forskningsansats	13
3.1.1 Varför denna fallstudie	13
3.1.2 Steg-för-steg-beskrivning av forskningsflödet	14
3.1.3 Hur EN 18031-metodiken följdes	14
3.1.4 TARA tillämpning och begränsning	15
3.1.5 Validitet och reliabilitet	15
3.1.6 Tillverkarsamarbetets metodologiska roll	15
3.1.7 Begränsningar och motivering	15
3.2 Litteraturstudie	15
3.3 Fallbeskrivning	16
3.4 Datainsamling	16
3.5 Säkerhetsanalys med EN 18031	17
3.6 Riskbedömning	18
3.6.1 Tillvägagångssätt och underlag	18
3.6.2 Identifiering av sårbarheter och hot	18
3.6.3 Riskbedömningsmetodik och riskmatris	21
4. Resultat	23
4.1 Beskrivning av analyserad enhet	23
4.2 Resultat från EN 18031-analysen	23
4.3 Identifierade risker	27
4.4 Förbättringsförslag	29
5. Diskussion	29

6.	Slutsats	31
7.	Framtida arbete	31
8.	Referenser	32
9.	Bilagor	34
	Bilaga 1. Sammanställning av bedömda krav	34
	Bilaga 1a. Uppfyllda krav (Pass) – 9 krav	34
	Bilaga 1b. Underkända krav (Fail) — 11 krav	35
	Bilaga 1c. Krav med avvikelse (Non-Conformity) — 19 krav.....	36
	Bilaga 1d. Ej tillämpliga krav (N/A) — 9 krav	38
	Bilaga 2. Tillgångsregister	39
	Bilaga 3. Mappning av tillgångar till hot och attackvektorer	40

1. Inledning

1.1 Kontext och motivering

Uppkopplade enheter, ofta kallade IoT-enheter, är i dag en integrerad del av moderna nätverk och används inom allt från smarta hem och industriell automatisering till ladd-infrastruktur för elfordon. I takt med att antalet uppkopplade enheter ökar, växer också attackytan för potentiella säkerhetshot. Till skillnad från traditionella datorsystem utvecklas IoT-enheter ofta med fokus på funktionalitet och kostnad snarare än säkerhet, vilket resulterar i återkommande säkerhetsbrister som svaga standardlösenord, okrypterad kommunikation och avsaknad av säkra uppdateringsmekanismer. [7] NIST SP 800-213 ger konkret vägledning till tillverkare om hur dessa brister bör hanteras genom strukturerade cybersäkerhetskrav. [1]

För att hjälpa tillverkare arbeta mer strukturerat med cybersäkerhet har den europeiska standarden EN 18031 tagits fram. Standarden erbjuder ett ramverk med tydliga krav och bedömningsmetoder för säkerhetsanalys av uppkopplade produkter [2]. Ämnet har blivit extra aktuellt i och med att Europeiska unionen inför Cyber Resilience Act (CRA), som från 2027 ställer bindande säkerhetskrav på produkter med digitala element som säljs inom EU. EN 18031 är en av de standarder som förväntas användas för att uppfylla dessa krav. [3]

För att konkretisera detta undersöks i arbetet hur EN 18031 kan användas vid analys av en verklig IoT-enhet, genomfört i samarbete med ett företag.

1.2 Problemformulering

EN 18031 är en relativt ny standard och kunskapen om hur den tillämpas i praktiken är fortfarande begränsad hos många tillverkare. Det räcker inte att enbart känna till standardens krav på en teoretisk nivå - för att kunna ta nödvändiga åtgärder behöver tillverkare konkreta exempel på hur standarden kan omsättas i praktisk säkerhetsanalys [5]. I takt med att CRA:s ikraftträdande närmar sig ökar behovet av denna kunskap ytterligare, eftersom bristande förberedelse riskerar att försena marknadstillträde eller resultera i produkter som inte uppfyller regulatoriska krav. Det här arbetet bidrar till den kunskapen genom att visa hur EN 18031 kan användas som ett strukturerat analysverktyg i en verklig produktkontext.

1.3 Syfte och frågeställningar

Syftet med detta arbete är att undersöka hur EN 18031 kan användas som ett strukturerat ramverk för säkerhetsanalys av en IoT-enhet i en praktisk kontext. Arbetet genomförs som en fallstudie i samarbete med ett företag, där en verklig IoT-enhet analyseras för att konkretisera och förstärka resultaten.

Följande frågeställningar vägleder arbetet:

- Vad kräver EN 18031 av en IoT-enhet?
- Hur kan EN 18031 tillämpas i praktiken på en verklig IoT-enhet?
- Hur kan EN 18031 användas som stöd inför framtida arbete med CRA?

1.4 Avgränsning

Arbetet fokuserar på EN 18031 som tekniskt ramverk och inkluderar inte juridisk tolkning av Cyber Resilience Act. Ingen formell produktcertifiering eller CE-märkning ingår i studien, och utveckling av nya IoT-produkter faller utanför ramen för detta arbete. CRA behandlas som bakgrundskontext för att motivera relevansen av EN 18031, men är inte föremål för djupanalys.

Vissa tekniska detaljer om den analyserade enheten redovisas inte fullt ut med hänsyn till konfidentialitet gentemot det berörda företaget. Detta påverkar detaljnivån i den offentliga redovisningen av teknisk evidens, men inte själva bedömningen av analyserade krav.

Samtliga krav som ingår i resultatredovisningen har därför klassificerats som Pass, Fail eller Non-Conformity, även om all bakomliggande teknisk information inte kan publiceras i full detalj. Studien är vidare avgränsad till en specifik IoT-produkt i en bestämd kontext, vilket innebär att resultaten inte är direkt generaliserbara till alla typer av IoT-enheter.

1.5 Disposition

Arbetet är strukturerat enligt följande. Kapitel 2 ger en teoretisk bakgrund till IoT-säkerhet, EN 18031 och Cyber Resilience Act. Kapitel 3 beskriver den metod som använts, inklusive forskningsansats, litteraturstudie, fallbeskrivning, datainsamling, riskbedömning och hur säkerhetsanalysen genomfördes. Kapitel 4 presenterar resultaten från analysen, inklusive en beskrivning av den analyserade enheten, EN 18031-bedömningen, identifierade risker och förbättringsförslag. Kapitel 5 diskuterar och tolkar resultat i relation till arbetets frågeställningar. Kapitel 6 presenterar arbetets slutsatser och kapitel 7 föreslår riktningar för framtida arbete. Arbetet avslutas med en referenslista samt bilagor.

2. Bakgrund

2.1 IoT-säkerhet

IoT-enheter är resursbegränsade system som ofta saknar de säkerhetsfunktioner som finns i traditionella datorsystem. Begränsningar i processorkraft, minne och energiförbrukning gör det svårt att implementera avancerade säkerhetslösningar, vilket skapar strukturella svagheter i många enheter. [7]

Forskning har identifierat flera återkommande säkerhetsbrister i IoT-produkter. Svaga eller förinställda lösenord som aldrig byts ut gör enheter enkelt åtkomliga för obehöriga. Okrypterad kommunikation innebär att data kan avlyssnas under överföring. Osäkra uppdateringsmekanismer möjliggör installation av manipulerad programvara. Bristande åtkomstkontroll tillåter obehöriga entiteter att komma åt enhetens funktioner och lagrade data. [4]

Dessa brister gör IoT-enheter till attraktiva mål för angripare och skapar risker som kan påverka både enskilda användare och bredare nätverksinfrastruktur. För att tillverkare systematiskt ska kunna identifiera och åtgärda dessa svagheter krävs ett strukturerat ramverk för säkerhetsanalys, något som EN 18031 är utformat att erbjuda.

2.2 EN 18031

EN 18031 är en europeisk standard som tagits fram för att ge tillverkare ett strukturerat ramverk för säkerhetsanalys av uppkopplade produkter. Standarden är uppdelad i tre delar: EN 18031-1 riktar sig mot internetanslutna enheter, EN 18031-2 mot enheter som hanterar persondata och EN 18031-3 mot enheter som hanterar finansiella transaktioner. En produkt kan omfattas av en eller flera delar beroende på dess funktion. [2]

Standarden är uppbyggd kring ett antal säkerhetsmoduler där varje modul adresserar ett specifikt säkerhetsområde. Bedömningen inom varje modul följer ett strukturerat beslutsträd där svaren avgör om ett krav är uppfyllt, delvis uppfyllt eller inte uppfyllt. Tabell 1 ger en översikt över standardens moduler. [6]

Tabell 1. Översikt över EN 18031: Säkerhetsmoduler. Egen sammanfattning baserad på [6].

Modul	Fullständigt namn	Beskrivning
ACM	Access Control Mechanism	Åtkomstkontroll till skyddade tillgångar
AUM	Authentication Mechanism	Autentisering och lösenordsskydd
SUM	Software Update Mechanism	Säkra programuppdateringar
SSM	Secure Storage Mechanism	Säker lagring av känsliga tillgångar
SCM	Secure Communication Mechanism	Krypterad och autentiserad kommunikation
LGM	Log Mechanism	Loggning av relevanta händelser
DLM	Deletion Mechanism	Radering av persondata och säkerhetsparametrar
UNM	User Notification Mechanism	Användarinformation om datainsamling

RLM	Resilience Mechanism	Motståndskraft mot överbelastningsattacker
NMM	Network Monitoring Mechanism	Nätverksövervakning
TCM	Traffic Control Mechanism	Trafikstyrning
CCK	Confidential Cryptographic Key	Kryptografiska nycklars styrka och unikheter
GEC	General Security	Övergripande säkerhetskrav
CRY	Cryptography	Kryptografi enligt bästa praxis

Genom att systematiskt gå igenom standardens moduler kan tillverkaren identifiera säkerhetsbrister och vidta åtgärder innan produkten når marknaden. EN 18031 fungerar därmed som ett praktiskt verktyg för strukturerad säkerhetsanalys av IoT-enheter.

EN 18031 är direkt kopplad till EU:s radioutrustningsdirektiv (RED), som sedan augusti 2025 ställer bindande cybersäkerhetskrav på radioutrustning via harmoniserade standarder. Eftersom den analyserade EV-laddaren kommunicerar via WiFi klassificeras den som radioutrustning under RED, vilket innebär att EN 18031 är tillämplig. Standarden täcker i detta fall alla tre relevanta delar: EN 18031-1 (internetanslutning), EN 18031-2 (persondata) och EN 18031-3 (finansiella transaktioner).

Tillverkare kan välja mellan självbedömning (self-assessment) eller certifiering via ett tredjepartsorgan som Nemko, Intertek, RISE eller TÜV. Vid självbedömning tar tillverkaren själv fram ett tekniskt underlag och bedömer att kraven är uppfyllda, vilket resulterar i CEmärkning. En tredjepartsgranskning innebär att ett ackrediterat organ granskar samma underlag oberoende. I båda fallen används EN 18031:s beslutsträd och bedömningsmall som metodologiskt verktyg. Den genomförda studien utgick från en självbedömningsliknande process, men med extern analytiker och i samarbete med tillverkaren.

2.3 Cyber Resilience Act

Cyber Resilience Act (CRA) är en EU-förordning som införs som svar på de ökande säkerhetsriskerna med uppkopplade produkter. Från 2027 ställer förordningen bindande krav på tillverkare av produkter med digitala element som säljs inom EU.

Förordningen kräver att tillverkare genomför och dokumenterar riskbedömning, hanterar sårbarheter aktivt under produktens livscykel och tillhandahåller säkerhetsuppdateringar under en definierad supportperiod. Tillverkare som inte uppfyller kraven riskerar att nekas marknadsstillträde inom EU. [3]

EN 18031 utgör därmed ett konkret förberedelsesteg för tillverkare som vill möta CRA:s krav. [8]

2.4 TARA och ISO/SAE 21434

TARA (Threat Analysis and Risk Assessment) är en strukturerad metodik för hotanalys och riskbedömning av inbyggda och uppkopplade system. Metodiken används för att systematiskt identifiera skyddsvärda tillgångar, kartlägga potentiella hot mot dessa tillgångar, analysera tänkbara attackvägar och slutligen bedöma och formellt poängsätta de risker som identifieras. Resultatet av en TARA-analys utgör ett beslutsunderlag för vilka säkerhetsåtgärder som bör implementeras med vilken prioritet. [18]

TARA är en central del av ISO/SAE 21434:2021, en internationell standard som reglerar cybersäkerhetsarbete inom fordonsindustrin. Standarden ställer krav på att tillverkare genomför strukturerade hotanalyser under hela produktens livscykel från konceptfas till avveckling eftersom fordonssystem i allt högre grad är uppkopplade och kommunicerar med externa tjänster har behovet av formaliserad hotmodellering ökat markant. ISO/SAE 21434 svarar på detta behov genom att definiera en process där TARA används som verktyg för att identifiera cybersäkerhetsrisker och fastställa acceptansnivåer för dessa. [18]

EN 18031 och TARA är komplementära metoder som angriper IoT-säkerhet från olika utgångspunkter. EN 18031 är ett kravbaserat ramverk som bedömer om en produkt uppfyller ett definierat set av säkerhetskrav organiserade i moduler. Fokus ligger på att fastställa efterlevnad om kravet är uppfyllt, delvis uppfyllt eller inte uppfyllt. TARA däremot är en hotmodellerings- och riskbedömningsmetod som utgår från tillgångarna och arbetar sig fram till konkreta attackscenarier med formell riskpoängsättning. Tillsammans ger metoderna en mer fullständig säkerhetsbild: EN 18031 identifierar regulatoriska gap och brister i implementationen, medan en TARA-analys kan förklara varför dessa gap utgör risker och hur allvarliga dessa risker är i praktiken.

2.5 Relaterat arbete

Forskningen kring IoT-säkerhet har under det senaste decenniet resulterat i ett antal ramverk, standarder och empiriska studier som är direkt relevanta för detta arbete. NIST identifierar i NISTIR 8228 [7] tre övergripande skillnader mellan IoT och traditionell IT: kopplingen till den fysiska världen, att många IoT-enheter inte kan nås, hanteras eller övervakas på samma sätt som konventionella IT-system, samt att säkerhetsfunktioner ofta fungerar annorlunda eller är mer begränsade i IoT-miljöer. Dessa grundläggande utmaningar bekräftas i den bredare forskningslitteraturen. Sadhu et al. [9] presenterar en omfattande kartläggning av säkerhetssårbarheter i IoT-system och identifierar återkommande brister som svaga lösenord, okrypterad kommunikation och osäkra firmware-uppdateringar som de vanligaste attackvektorerna. Sebestyen et al. [10] bekräftar i en systematisk litteraturöversikt att otillräcklig kryptering och bristande autentiseringsmekanismer konsekvent identifieras som de allvarligaste sårbarheterna i IoT-produkter, ett mönster som återkommer oberoende av enhetstyp och bransch.

Autentiseringsproblematiken i IoT-enheter har studerats ingående ur ett protokollperspektiv. Luo et al. [11] visar i en systematisk genomgång av IoT-autentiseringsprotokoll att många befintliga lösningar saknar tillräcklig motståndskraft mot brute force-attacker och att avsaknaden av tvåfaktorsautentisering är ett genomgående problem. Dessa slutsatser stöds av en bredare systematisk litteraturoversikt av Neshenko et al. [12], som konstaterar att autentisering och kryptering konsekvent utgör de svagaste länkarna i IoT-säkerhetsarkitekturer. ENISA:s rapport om IoT-säkerhetsstandarder [5] bekräftar att det inte finns något signifikant gap i standarder för att uppfylla enskilda säkerhetskrav, men att det finns ett tydligt gap i processen för hur en tillverkare faktiskt ska kunna visa att en IoT-produkt är säker.

Kommunikationsprotokollets säkerhet är en central fråga för uppkopplade enheter som kommunicerar via internet. Paris et al. [13] har experimentellt undersökt implementationen av SSL/TLS-kryptering i kombination med MQTT-protokollet på ESP32-baserade enheter och visar att kryptering visserligen medför ökad energiförbrukning men är genomförbar även på resursbegränsade enheter. Detta är direkt relevant för EV-laddare och liknande IoT-enheter som förlitar sig på MQTT för fjärrkommunikation.

Inom det specifika området EV-laddarsäkerhet har Johnson et al. [14] genomfört en ingående granskning av cybersäkerhetssårbarheter i laddinfrastruktur, kategoriserat sårbarheterna efter gränssnittstyp och visat att attacker kan riktas mot enhetens kommunikationsprotokoll, molnbackend, betalningssystem och fysiska gränssnitt. Alcaraz et al. [15] kompletterar detta med en djupanalys av säkerhetshot mot OCPP-protokollet och visar att OCPP i sin grundkonfiguration är sårbart för bland annat man-in-the-middle-attacker, falsk datainjektion och denial-of-service, med potentiella konsekvenser för både enskilda laddstationer och det bredare elnätet.

Ur ett regulatoriskt perspektiv analyserar Eckhardt och Kotovskaia [16] hur EU:s Cyber Resilience Act (CRA), som trädde i kraft den 10 december 2024 med huvudsaklig tillämpning från den 11 december 2027, interagerar med befintlig cybersäkerhetslagstiftning och klargör att tillverkare av produkter med digitala element är skyldiga att genomföra riskbedömningar och vidta konkreta säkerhetsåtgärder. NIST [17] har tagit fram vägledning specifikt riktad till IoT-tillverkare, med rekommendationer om hur grundläggande cybersäkerhetsaktiviteter bör integreras i produktutvecklingen. Sammantaget visar den befintliga forskningen att de sårbarhetsmönster som identifierats i detta arbete — osäker kommunikation, bristande uppdateringsmekanismer, svag lagringssäkerhet och otillräcklig autentisering — är väldokumenterade inom både IoT-säkerhet generellt och EV-laddinfrastruktur specifikt. Strukturerade ramverk för säkerhetsanalys, som EN 18031, fyller därmed ett tydligt behov hos tillverkare som behöver ett praktiskt och reproducerbart verktyg för att identifiera och åtgärda säkerhetsbrister i sina produkter.

Ett närliggande standardiseringsspår som också är relevant för detta arbete är ETSI EN 303 645, som utgör en etablerad europeisk cybersäkerhetsstandard för konsumentnära IoT-produkter. Standarden har fått stor betydelse som ett tidigt praktiskt ramverk för grundläggande säkerhetskrav, exempelvis inom lösenordshantering, säker uppdatering, sårbarhetshantering och skydd av kommunikation. EN 18031 kan i detta sammanhang förstås

som ett mer formellt och regulatoriskt relevant bedömningsramverk för produkter som ska utvärderas i relation till EU:s cybersäkerhetskrav, samtidigt som den i stor utsträckning harmoniserar med principer som återfinns i ETSI EN 303 645. Därför är studier av EN 18031:s praktiska tillämpning också relevanta i ett bredare standardiseringsperspektiv, eftersom de visar hur tidigare vägledande säkerhets-principer kan omsättas i en mer strukturerad krav- och bedömningsmodell.

3. Metod

3.1 Forskningsansats

Detta arbete är utformat som en kvalitativ fallstudie baserad på analys av en verklig IoT-enhet. En kvalitativ ansats lämpar sig när syftet är att förstå och beskriva ett fenomen i sin kontext snarare än att mäta det numeriskt. Eftersom arbetet syftar till att undersöka hur EN 18031 konkret kan tillämpas på en verklig produkt bedöms denna ansats som mest ändamålsenlig.

Fallstudien möjliggör en djupgående och kontextuell analys som bidrar till förståelsen av hur standarden fungerar i praktiken - något som är svårt att uppnå med bredare eller mer generella metoder.

3.1.1 Varför denna fallstudie

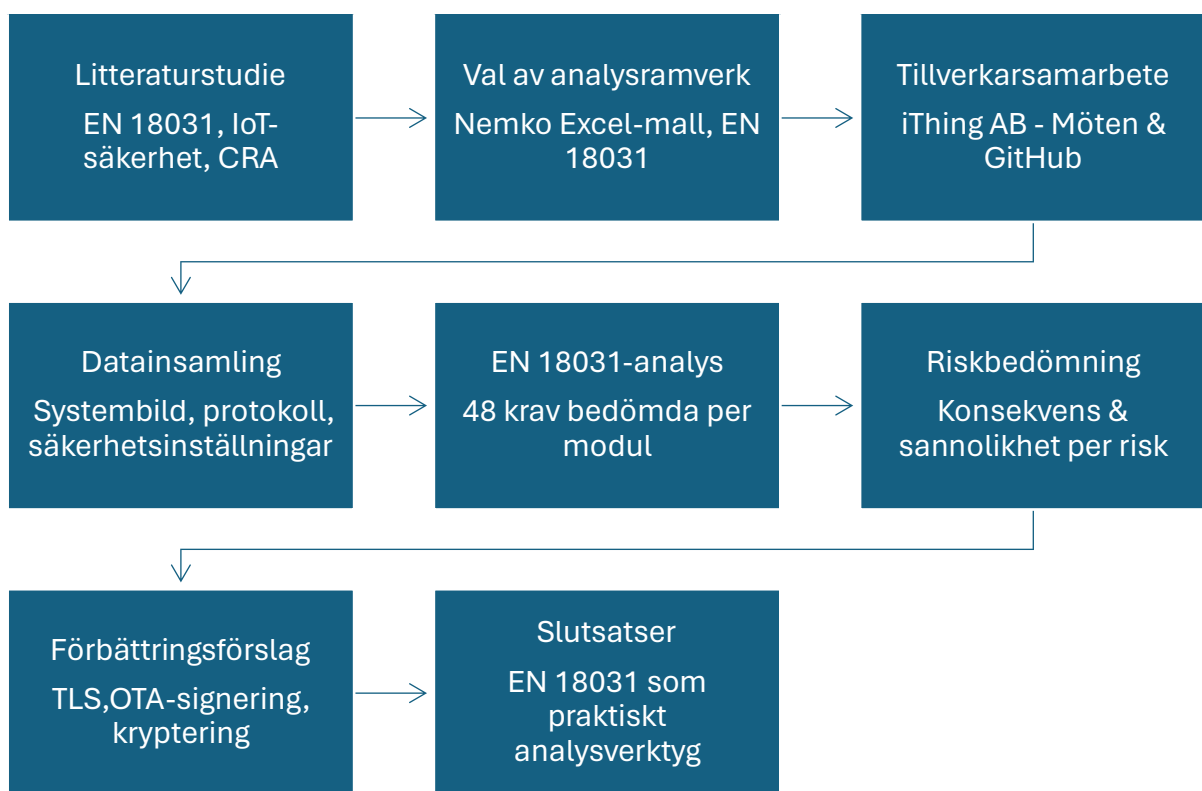
En fallstudie valdes eftersom syftet är att undersöka hur EN 18031 fungerar i en verklig produktkontext, inte att mäta fenomenet över ett stort urval. En EV-laddare är ett lämpligt studieobjekt eftersom den omfattas av samtliga tre delar av EN 18031, vilket ger en bred och representativ analys av standardens tillämpbarhet. Samarbetet med iThing AB, möjliggjorde tillgång till teknisk information som annars inte hade varit tillgänglig för extern analys.

EN 18031 omfattar sammantaget ett större antal krav och delkrav än vad som är relevant att analysera för varje enskild produkt. I den fullständiga standardstrukturen kan det röra sig om omkring 70–80 krav beroende på hur huvudkrav, underkrav och produktspecifika tillämpningar räknas. I denna studie analyserades 48 krav, eftersom urvalet avgränsades till de krav som var relevanta för den undersökta EV-laddarens faktiska funktioner, exponeringar och tillgångar. Krav som avsåg funktioner eller mekanismer som inte används av produkten, eller som bedömdes som inte tillämpliga i just denna produktkontext, exkluderades från den detaljerade analysen. Relevansbedömningen gjordes med stöd av standardens modulstruktur, Nemkos bedömningsmall samt dialog med tillverkaren, vilket även möjliggjorde rimlig avstämning av urvalet mot hur en extern granskare skulle kunna bedöma tillämpligheten.

3.1.2 Steg-för-steg-beskrivning av forskningsflödet

Arbetet följde ett strukturerat flöde från litteraturstudie till slutsatser. Processen inleddes med en genomgång av befintlig forskning inom IoT-säkerhet och EN 18031 följt av val av analysramverk och bedömningsverktyg. Därefter genomfördes datainsamling i samarbete med tillverkaren, varpå EN 18031 analysen utfördes systematiskt modul för modul. Analysen låg sedan till grund för riskbedömning och förbättringsförslag, som sammantaget ledde fram till arbetets slutsatser. Se figur 1 för flödesschema.

Figur 1. Forskningsprocessens arbetsflöde



3.1.3 Hur EN 18031-metodiken följdes

Analysen följde standardens inbyggda bedömningsstruktur. För varje säkerhetsmodul granskades relevanta krav med hjälp av Nemkos Excel-baserade bedömningsverktyg, som innehåller standardens beslutsträd och utvärderingsfrågor. Varje krav bedömdes som Pass, Non-Conformity eller Fail baserat på information från tillverkaren. Tillvägagångssättet säkerställde att analysen var systematisk och reproducerbar.

3.1.4 TARA tillämpning och begränsning

En fullständig TARA-analys genomfördes inte inom ramen för detta arbete. Metodikens formella riskpoängsättning och strukturerade attackmodellering kräver tillgång till detaljerad internteknisk dokumentation samt ett dedikerat analysarbete som går utöver vad denna studie syftade till. Däremot tillämpades TARA:s grundprinciper informellt: tillgångar identifierades systematiskt, potentiella hot kartlades per tillgång och konsekvenser av identifierade brister beskrevs. Dessa moment utgör kärnan i TARA-metodiken och präglade analysarbetet även om ingen formell riskpoäng beräknades

3.1.5 Validitet och reliabilitet

Analysens validitet stärktes genom att bedömningarna baserades direkt på EN18031:s egna bedömningskriterier snarare än på subjektiva uppskattningar. Reliabiliteten säkerställdes genom att samma strukturerade bedömningsverktyg användes konsekvent för samtliga krav, och att oklarheter följdes upp skriftligen via GitHub mellan mötena med tillverkaren. Att analysen genomfördes av en enskild bedömare, utan extern verifiering, utgör en begränsning, men den strukturerade metodiken minskar risken för godtyckliga bedömningar.

3.1.6 Tillverkarsamarbetets metodologiska roll

Samarbetet med iThing AB var en förutsättning för analysens genomförande. EN 18031 förutsätter tillgång till intern teknisk dokumentation för att bedömningar ska kunna göras korrekt, och flera krav hade inte kunnat bedömas utan tillverkarens direkta input. Detta innebär att analysen är beroende av att tillverkarens uppgifter är korrekta, vilket är en metodologisk begränsning som beskrivs närmare nedan.

3.1.7 Begränsningar och motivering

Studien är begränsad till en enskild IoT-enhet i samarbete med ett specifikt företag, vilket innebär att resultaten inte är direkt generaliserbara till andra produkttyper eller tillverkare. Analysen baserades på tillverkarens uppgifter utan möjlighet till oberoende teknisk verifiering. Trots dessa begränsningar är ansatsen ändå lämplig för studiens syfte: att konkret visa hur EN 18031 kan tillämpas i praktiken och vilka säkerhetsbrister en sådan analys kan identifiera

3.2 Litteraturstudie

Arbetet inleds med en litteraturstudie i syfte att bygga en teoretisk grund för analysen. Standarddokumentet EN 18031 har studerats i sin helhet för att förstå standardens krav och bedömningsmetodik. Befintlig forskning inom IoT-säkerhet har använts för att förstå vilka säkerhetsbrister som är vanligt förekommande i uppkopplade produkter. ENISA:s rapport om IoT-säkerhet lyfter fram svaga lösenord och okrypterad kommunikation som exempel på

sådana risker.[5] Cyber Resilience Act har studerats som bakgrundskontext för att motivera relevansen av EN 18031.

Som tekniskt underlag för analysen användes ett strukturerat bedömningsdokument i form av en Excel-mall baserad på EN 18031, ursprungligen framtagen av Nemko som ett standardiserat bedömningsverktyg och tillhandahållen av iThing AB. Mallen innehåller standardens samtliga krav organiserade per säkerhetsmodul. Varje krav granskades och resultatet dokumenterades som Pass, Non-Conformity eller Fail. Mallens inbyggda utvärderingsfrågor per krav fungerade som utgångspunkt för att identifiera informationsluckor, vilket ledde till mer specifika tekniska frågor som ställdes vid det fysiska mötet med iThing AB.

3.3 Fallbeskrivning

Arbetet genomfördes i samarbete med iThing AB. Den analyserade enheten är en uppkopplad EV-laddare som används i en kommersiell kontext. En uppkopplad EV-laddare hanterar finansiella transaktioner, persondata och kritisk styrfunktionalitet via internet, vilket gör den till ett potentiellt mål för cyberattacker och motiverar behovet av en strukturerad riskanalys.

Av konfidentialitetsskäl redovisas inte alla tekniska detaljer om enhetens implementation och säkerhetskonfiguration i detta arbete, i enlighet med avgränsningarna i avsnitt 1.4. Analysen genomfördes utan fullständig direkt fysisk eller nätverksbaserad teståtkomst till enheten. Det tekniska underlaget bestod i stället av systembeskrivningar, kommunikationsprotokoll, säkerhetsinställningar, arkitekturbeskrivningar och kompletterande uppgifter från tillverkaren, vilka samlades in genom fysiska möten och efterföljande skriftlig uppföljning.

Bedömningarna grundades därmed på dokumentationsgranskning, genomgång av produktens kommunikationsflöden och systematiskt jämförande mot EN 18031:s kravstruktur. Detta innebär att arbetet inte utgjorde en fullständig penetrationstestning, men väl en strukturerad kravbaserad säkerhetsanalys av produktens nuvarande säkerhetsstatus.

3.4 Datainsamling

Datainsamlingen genomfördes under en period av cirka fem veckor med veckovisa fysiska möten med representanter från iThing AB samt kompletterande skriftlig uppföljning mellan mötena. Under det inledande arbetet upprättades gemensamt en övergripande systembild av EV-laddaren, där kommunikationsflöden, nätverksgränssnitt, centrala systemkomponenter och relevanta tillgångar identifierades. Tillverkaren beskrev därefter hur enheten kommunicerar med externa tjänster, vilka säkerhetsmekanismer som fanns implementerade samt hur autentisering, lagring, uppdatering och extern kommunikation hade utformats. Detta utgjorde det primära empiriska underlaget för den fortsatta EN 18031-analysen.

Datainsamlingen syftade inte enbart till att samla tekniska fakta om produkten, utan även till att möjliggöra identifiering av säkerhetsrelevanta tillgångar, hot, sårbarheter och möjliga attackvektorer. Dessa identifierades genom en kombination av dokumentationsgranskning, genomgång av systemarkitektur och kommunikationsprotokoll, analys av konfigurations- och

säkerhetsuppgifter från tillverkaren samt jämförelse med EN 18031:s krav och etablerade sårbarhetsmönster i litteraturen. Eftersom studien inte omfattade fullständig penetrationstestning eller egen verifiering mot specifika CVE-poster identifierades sårbarheter inte genom aktiv exploatering, utan genom kravbaserad analys av kända riskområden såsom okrypterad kommunikation, bristande lagringsskydd, otillräcklig autentisering och osäker uppdateringshantering. Mellan mötena användes GitHub som kommunikationskanal för att följa upp oklarheter och komplettera underlaget, vilket bidrog till att analysen kunde genomföras systematiskt och spårbart.

3.5 Säkerhetsanalys med EN 18031

Analysen inleddes med att kartlägga EV-laddarens funktioner, nätverksgränssnitt och tillgångar. Tillgångarna identifierades baserat på EN 18031:s definitioner för säkerhets-, nätverks- och finansiella tillgångar, i kombination med information från det fysiska mötet med tillverkaren. Totalt identifierades nio aktiva tillgångar: Start/Stoppladdning, fordonskommunikation, firmware, NVS-Flash, autentiseringsuppgifter, lösenord, OCPP 1.6, MQTT samt interna energidata. Se Bilaga 2.

Därefter identifierades potentiella hot, sårbarheter och möjliga attackvektorer för varje tillgång, baserat på teknisk dokumentation, genomgång av enhetens arkitektur och kommunikationsflöden samt information om implementerade säkerhetslösningar från tillverkaren. Med detta som grund kontrollerades enheten systematiskt mot relevanta moduler och krav i EN 18031, där endast de krav som bedömdes som tillämpliga för den analyserade EV-laddarens funktioner, gränssnitt och användningskontext inkluderades i den detaljerade analysen. Totalt analyserades 48 krav. Övriga krav bedömdes som inte tillämpliga för produkten och klassificerades därför som N/A.

Resultatet av varje kontroll dokumenterades enligt bedömningskategorierna Pass, Fail och Non-Conformity. Pass innebär att det tillgängliga underlaget bedömdes vara tillräckligt för att kravet skulle anses uppfyllt. Fail innebär att det tillgängliga underlaget visade tydliga brister i förhållande till kravet. Non-Conformity innebär att kravet ännu inte kunde bedömas som uppfyllt fullt ut, exempelvis därför att implementationen inte var färdig, att kompletterande åtgärder återstod eller att underlaget ännu inte var tillräckligt för ett Pass. Skillnaden mellan Fail och Non-Conformity är därmed att Fail användes när den genomförda analysen visade att kravet inte var uppfyllt i produktens nuvarande utformning, medan Non-Conformity användes när kravet ännu inte kunde bedömas som uppfyllt men där fortsatt arbete, komplettering eller färdigställande återstod.

3.6 Riskbedömning

Riskbedömningen i studien genomfördes som en kvalitativ analys baserad på resultaten från EN 18031-bedömningen. Syftet var att tolka hur identifierade brister, avvikelser och ofullständigheter kunde påverka den analyserade EV-laddarens säkerhet, funktion och skydd av data. Bedömningen utgjorde därmed inte en formell kvantitativ riskanalys, utan en strukturerad tolkning av vilka säkerhetsmässiga konsekvenser de identifierade bristerna kunde medföra i produktens nuvarande utformning.

Som underlag för riskbedömningen användes de tillgångar som identifierades i avsnitt 3.5, tillsammans med systemarkitektur, kommunikationsvägar, nätverksgränssnitt, teknisk dokumentation och information från tillverkaren om implementerade säkerhetsmekanismer. Genom att koppla dessa till EN 18031:s kravområden kunde potentiella risker identifieras inom exempelvis kommunikationsskydd, autentisering, säker lagring, uppdateringshantering, loggning och tillgänglighet.

3.6.1 Tillvägagångssätt och underlag

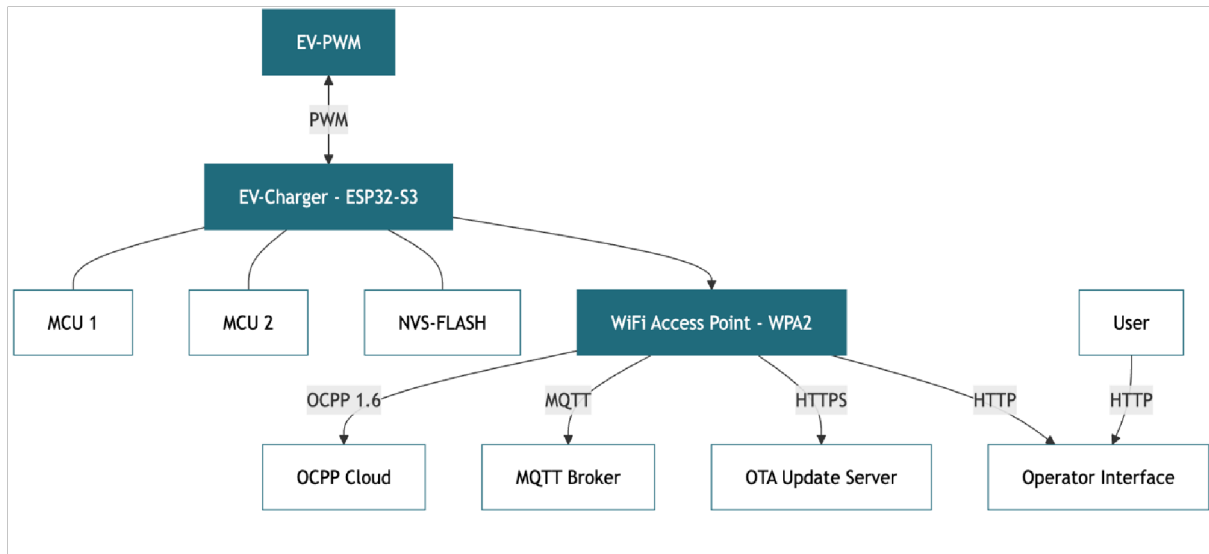
Riskerna identifierades genom att analysera vilka konsekvenser som kunde följa av krav som bedömts som Fail eller Non-Conformity. I denna analys beaktades särskilt om en brist kunde möjliggöra obehörig åtkomst, manipulation av data eller funktioner, avlyssning av kommunikation, installation av otilåten programvara, bristande spårbarhet vid incidenter eller påverkan på enhetens tillgänglighet. På detta sätt användes EN 18031 inte enbart som ett verktyg för kravgranskning, utan också som ett stöd för att identifiera och strukturera produktens centrala säkerhetsrisker.

3.6.2 Identifiering av sårbarheter och hot

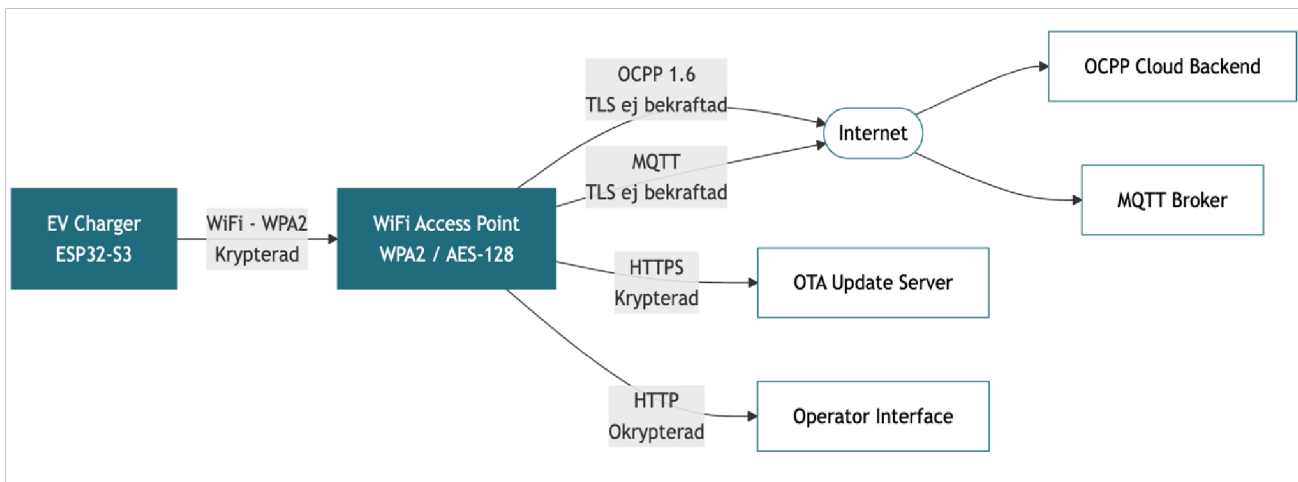
Det bör noteras att riskidentifieringen inte baserades på aktiv exploit-testning, penetrationstestning eller sökning mot specifika CVE-poster för de ingående komponenterna. Sårbarheter och hot identifierades i stället genom den kravbaserade analysen av kända riskområden — okrypterad kommunikation, bristande lagringsskydd, otillräcklig autentisering och osäker uppdateringshantering — i kombination med etablerade sårbarhetsmönster från litteraturen inom IoT-säkerhet och EV-laddinfrastruktur.

Systemarkitekturen och kommunikationsflödena som låg till grund för tillgångskartläggningen och riskbedömningen åskådliggörs i Figur 2 (systemarkitektur) och Figur 3 (nätverkskommunikation och protokoll).

Figur 2. Systemarkitektur för den analyserade EV-laddaren



Figur 3. Nätverkskommunikation och protokoll



Bedömningsprocessen för varje krav i EN 18031 följde ett strukturerat flöde i tre steg: tillgångskartläggning, beslutsträdsgenombgång och utfallsdokumentation. Nedan illustreras denna process med konkreta exempel från den genomförda analysen. Samma tillvägagångssätt tillämpades systematiskt för samtliga 48 analyserade krav, fördelade över standardens moduler och tillgångar.

I det första steget identifierades vilka tillgångar som var relevanta för det aktuella kravet. EN 18031 skiljer mellan säkerhetstillgångar (security assets), nätverkstillgångar (network assets) och finansiella tillgångar (financial assets), och bedömningen av ett krav måste göras separat för varje berörd tillgång. Som exempel krävde kravet ACM-1 (åtkomstkontroll) att analysera varje identifierad tillgång individuellt — firmware, NVS-Flash, autentiseringsuppgifter, OCPP 1.6, MQTT och interna energidata — för att avgöra om åtkomstkontroll fanns på plats för just den tillgången. Utan denna initiala kartläggning hade det inte gått att avgöra om kravet var tillämpligt eller hur det skulle bedömas.

I det andra steget ställde bedömningsmallen en sekvens av konkreta ja/nej-frågor, benämnda Decision Nodes (DN-1 till DN-5), till tillverkaren. Svarsvägen genom dessa noder bestämde utfallet för varje krav. För kravet SCM-1 (kommunikationsskydd) löd den centrala frågan om kommunikationen mellan enheten och molntjänsten skyddas med en godkänd krypteringsmetod. Om tillverkaren svarade ja och kunde påvisa hur krypteringen var implementerad, resulterade det i Pass. I det aktuella fallet visade tillverkarens svar att TLS inte var bekräftat implementerat på OCPP-kanalen, och någon tillräcklig riskjustifiering för varför okrypterad kommunikation var acceptabel gavs inte. Kravet resulterade därför i Fail. Mallen accepterar inte att ett protokoll bara används — den kräver att transporten är skyddad, eller att tillverkaren formellt motiverar varför ett undantag är försvarbart i den aktuella produktkontexten.

Samma logik tillämpades på MQTT-kommunikationen. Kravet SCM-2 frågade om kommunikationen mellan enheten och MQTT-brotern skyddas med godkänd krypteringsmetod. Tillverkarens svar visade att TLS inte var bekräftat implementerat på MQTT-kanalen, och ingen tillräcklig riskjustifiering gavs för varför okrypterad kommunikation var acceptabel. Även detta krav resulterade i Fail. Processen var densamma för SCM-3 och SCM-4, vilket innebar att samtliga fyra krav inom SCM-modulen bedömdes som Fail — ett resultat som tydligt synliggjorde att kommunikationsskyddet utgjorde ett prioriterat bristområde i produktens nuvarande utformning.

För AUM-kraven (autentisering) tillämpades beslutsträdet på liknande sätt, men med en mer uppdelad kravstruktur. Kravet AUM-5 var exempelvis uppdelat i underkraven AUM-5-1 och AUM-5-2. AUM-5-1 frågade om lösenordet är unikt per enhet — tillverkaren bekräftade detta, vilket resulterade i Pass. AUM-5-2 frågade om lösenordet är provisionerat av en auktoriserad tillverkare vid tillverkning — även detta bekräftades, och kravet resulterade i Pass. Däremot frågade AUM-4 om enheten har skydd mot upprepade inloggningsförsök, exempelvis i form av kontolåsning eller inloggningsfördröjning. Tillverkaren uppgav att denna funktion ännu inte var färdigimplementerad. Eftersom kravet varken kunde bedömas som uppfyllt eller som ett definitivt Fail — implementationen pågick men var inte slutförd — resulterade AUM-4 i Non-Conformity. Kravet AUM-1-1, som rör verifiering av identiteten hos anslutande användare och system, visade däremot tydliga brister i produktens nuvarande utformning och bedömdes som Fail.

I det tredje steget dokumenterades utfallet med en skriftlig motivering för varje krav. Bedömaren angav vilket underlag som låg till grund för bedömningen och varför kravet klassificerades som Pass, Fail eller Non-Conformity. För Non-Conformity-krav specificerades dessutom vad som återstod för att kravet i ett senare skede skulle kunna uppnå

Pass — exempelvis att en specifik mekanism ännu inte var implementerad, att dokumentation saknades, eller att kompletterande teknisk information behövde inhämtas från tillverkaren.

Denna trestegsprocess — tillgångskartläggning, beslutsträdsgenomgång och utfallsdokumentation — tillämpades konsekvent för samtliga 48 analyserade krav fördelade över modulerna ACM, AUM, SUM, SSM, SCM, RLM, CCK, GEC, LGM, DLM, UNM och CRY. Exemplen ovan är representativa för hur processen såg ut, men varje krav och tillgångskombination genomgick sin egen individuella bedömning baserad på det underlag som tillverkaren tillhandahöll. Processen synliggjorde inte enbart tekniska brister, utan också var tillverkaren saknade formell riskjustifiering, färdig implementation eller tillräcklig dokumentation. EN 18031 fungerade på så vis inte enbart som en checklista, utan som ett strukturerat analysinstrument som systematiskt tvingade fram svar på varför ett visst skydd inte finns — och huruvida tillverkaren överhuvudtaget hade reflekterat kring riskerna med det valet. Resultaten av riskbedömningen, inklusive de identifierade riskerna och deras koppling till specifika Fail- och Non-Conformity-utfall, presenteras i avsnitt 4.3.

3.6.3 Riskbedömningsmetodik och riskmatris

För att strukturera riskbedömningen användes en kvalitativ 3×3-matris baserad på två dimensioner: sannolikhet och konsekvens. Sannolikhet avser hur troligt det är att en identifierad brist faktiskt utnyttjas, givet produktens tekniska utformning och driftsmiljö. Konsekvens avser vilken påverkan ett lyckat utnyttjande skulle ha på produktens säkerhet, funktion eller skydd av data. Varje dimension bedömdes på en tregradig skala: Låg, Medelhög eller Hög.

Den kvalitativa riskbedömningsmetodiken följer principerna i NIST SP 800-30, som definierar ett ramverk för informationssäkerhetsriskbedömning baserat på sannolikhet och konsekvens som bedömningsdimensioner. [19]

Bedömningen av sannolikhet grundades på tre faktorer: om attackvektorn är nätverksåtkomlig eller kräver fysisk närvaro, om autentisering eller särskild kompetens krävs för att genomföra attacken, samt om liknande attacker är väldokumenterade i litteraturen för IoT-enheter eller EV-laddinfrastruktur. Bedömningen av konsekvens grundades på vilken typ av tillgång som påverkas, om bristen kan leda till obehörig åtkomst till styrsystem eller finansiella data, samt om bristen försvårar upptäckt eller utredning av incidenter.

Tabellerna 2 och 3 nedan visar riskmatrisen respektive de sju identifierade riskernas placering baserat på dessa bedömningar.

Tabell 2. Riskmatris — sannolikhet × konsekvens

	Konsekvens: Låg	Konsekvens: Medelhög	Konsekvens: Hög
Sannolikhet: Hög	Medel	Hög	Kritisk
Sannolikhet: Medelhög	Låg	Medel	Hög
Sannolikhet: Låg	Låg	Låg	Medel

Tabell 3. Riskplacering per identifierad risk

Risk	Sannolikhet	Konsekvens	Risiknivå
Okrypterad kommunikation	Hög	Hög	Kritisk
Brister i uppdatering	Medelhög	Hög	Hög
Otillräcklig intern lagring	Medelhög	Hög	Hög
Brister i autentisering	Hög	Hög	Kritisk
Begränsad loggning	Låg	Medelhög	Låg
Saknad återställningsmekanism	Medelhög	Hög	Hög
Saknad nätverksmotståndskraft	Medelhög	Hög	Hög

De två riskerna på kritisk nivå — okrypterad kommunikation och brister i autentiseringsmekanismen — bör prioriteras för åtgärd eftersom de kombinerar hög sannolikhet med hög konsekvens och är direkt nätverksåtkomliga utan krav på fysisk närvaro.

4. Resultat

4.1 Beskrivning av analyserad enhet

Den analyserade enheten är en uppkopplad EV-laddare avsedd för kommersiellt bruk. Enheten kommunicerar via WiFi med externa molntjänster och stöder fjärrstyrning samt OTA-uppdateringar. Kommunikationslänken benämns Air Link och möjliggör OCPP- och MQTT-kommunikation med molntjänster. Känsliga data lagras i enhetens interna minne. Enheten omfattas av EN 18031-1, EN 18031-2 och EN 18031-3 då den är internetansluten, hanterar persondata och är kopplad till finansiella transaktioner. För en fullständig beskrivning av studiekontexten och konfidentialitetsbegränsningar, se avsnitt 3.3.

4.2 Resultat från EN 18031-analysen

Tabell 4. Uppfyllda krav (pass).

De krav som bedömdes som Pass var sådana där det tillgängliga underlaget, i form av systemgenomgång, dokumentation och information från tillverkaren, visade att produktens nuvarande utformning motsvarade det aktuella kravet i EN 18031. Som framgår av Tabell 4 avsåg detta främst grundläggande krav inom autentisering, lösenordsunikhet, förekomst av uppdateringsmekanism, viss kryptografisk miniminivå i Wi-Fi-skyddet, motiverade fysiska gränssnitt samt persistent intern logglagring.

krav	Observation	Bedömning	Säkerhetspåverkan
AUM 1-2	Åtkomst via användargränssnitt kräver autentisering med användarnamn och lösenord	Pass	Skyddar mot obehörig åtkomst via användargränssnitt
AUM 2-1	Minst en autentiseringsfaktor används - lösenord utgör kunskapsfaktor	Pass	Grundläggande autentiseringskrav uppfyllt

AUM 3	Autentisering valideras server – sidan för samtliga kommunikationsmekanismer	Pass	Säkerställer att autentisering inte kan kringgås lokalt
AUM 5-1	Lösenord är unikt per enhet	Pass	Förhindrar att ett läckt lösenord komprometterar flera enheter
AUM 5-2	Lösenord provisionerat av auktoriserad tillverkare vid tillverkning	Pass	Säkerställer att lösenord sätts av behörig part
SUM 1	Uppdateringsmekanismen	Pass	Möjliggör att säkerhetsuppdateringar kan distribueras
CCK 1	Wi-Fi WPA2 använder AES-128 som uppfyller minimikravet på 112-bitars säkerhetsstyrka	Pass	Förhindrar att en komprometterad nyckel påverkar andra enheter
GEC 5	Fysiskt gränssnitt är nödvändig för enhetens avsedda funktion	Pass	Fysiska gränssnitt är motiverade och nödvändiga
LGM 2	Loggdata lagras i persistent intern lagring som behåller data vid omstart	Pass	Säkerställer att loggdata finns tillgänglig efter händelser

Tabell 5. Underkända krav (Fail)

De krav som bedömdes som Fail var i stället sådana där den genomförda analysen visade tydliga brister i förhållande till EN 18031:s krav för den aktuella produkten. Bedömningen grundades på den systematiska jämförelsen mellan produktens beskrivna säkerhetslösningar, kommunikationsflöden, lagringsmekanismer, uppdateringshantering och åtkomstrelaterade funktioner å ena sidan, och standardens krav å den andra. Som framgår av Tabell 5 gällde dessa brister framför allt åtkomstkontroll, identitetsverifiering, säker uppdatering, skydd av intern lagring, skydd av kommunikation samt kryptografisk tillämpning.

Krav	Observation	Bedömning	Säkerhetspåverkan
ACM-1	Åtkomstkontroll till skyddade funktioner uppfyller inte kravet fullt ut i produktens nuvarande utformning.	Fail	Ökar risken för obehörig åtkomst till skyddade funktioner och resurser.
AUM 1-1	Verifiering av identiteten hos anslutande användare eller system uppfyller inte kravet fullt ut.	Fail	Ökar risken för att obehöriga aktörer kan ansluta eller få åtkomst till funktioner.

SUM-2	Uppdateringsmekanismen uppfyller inte kravet på tillräckligt skydd mot osäker eller manipulerad firmware.	Fail	Ökar risken för installation av obehörig eller manipulerad programvara.
SSM-1, SSM-2, SSM-3	Skyddet av känsliga data i intern lagring uppfyller inte standardens krav fullt ut.	Fail	Ökar risken för att autentiseringsuppgifter, konfigurationsdata eller annan känslig information exponeras eller extraheras.
SCM-1, SCM-2, SCM-3, SCM-4	Kommunikationsskyddet uppfyller inte kraven för säker överföring mellan enheten och externa tjänster.	Fail	Ökar risken för avlyssning, manipulation av trafik och exponering av känsliga uppgifter.
CRY-1	Användningen av kryptografiska skyddsmekanismer uppfyller inte kravet på bästa praxis fullt ut.	Fail	Försvagar skyddet av kommunikation och data samt ökar risken för säkerhetsbrister i kryptografiska funktioner.

Tabell 5 redovisar därmed de krav där analysen visade att produktens nuvarande utformning inte uppfyllde det aktuella kravet. Fail-utfallen ska förstås som identifierade säkerhetsbrister i produktens nuvarande utvecklingsläge, inte som en fullständig certifieringsbedömning av hela produkten. Samtidigt är de metodiskt viktiga eftersom de visar hur EN 18031 i praktiken kan användas för att synliggöra konkreta gap mellan en produkts befintliga säkerhetsutformning och de krav som behöver vara uppfyllda inför framtida regulatorisk granskning.

Tabell 6. Krav bedömda som Non-Conformity

Modul	Krav-ID	Kravet avser	Bedömning
ACM	ACM-2	Åtkomstkontroll till skyddade funktioner och resurser	Non-Conformity
AUM	AUM-4, AUM-6	Ytterligare autentiseringsrelaterade kontroller	Non-Conformity
SUM	SUM-3	Ytterligare krav kopplade till uppdateringshantering	Non-Conformity
RLM	RLM-1	Motståndskraft mot nätverksrelaterade störningar	Non-Conformity
CCK	CCK-2, CCK-3	Krav kopplade till kryptografiska nycklar och relaterade skyddsmekanismer	Non-Conformity
GEC	GEC-1, GEC-3, GEC4, GEC-6, GEC-7, GEC-8	Övergripande säkerhetskrav	Non-Conformity

LGM	LGM-1, LGM-3, LGM-4	Ytterligare krav kopplade till loggning och logghantering	Non-Conformity
DLM	DLM-1	Radering av data och säkerhetsparametrar	Non-Conformity
UNM	UNM-1, UNM-2	Användarinformation om datainsamling och relaterade mekanismer	Non-Conformity

Utöver de krav som bedömdes som Pass eller Fail klassificerades en tredje grupp krav som Non-Conformity. Denna kategori användes för krav där analysen visade att produkten ännu inte kunde bedömas som uppfyllande i sin nuvarande utformning, men där bristen samtidigt inte bedömdes på samma definitiva sätt som de krav som klassificerades som Fail. För den analyserade EV-laddaren avsåg detta främst krav där implementationen ännu inte var färdigställd, där kompletterande funktioner eller säkerhetsåtgärder återstod, eller där produkten fortfarande befann sig i ett utvecklingsläge där full överensstämmelse ännu inte hade uppnåtts. Non-Conformity ska därför förstås som identifierade avvikelser och kvarstående utvecklingspunkter i relation till EN 18031, snarare än som uppfyllda krav eller slutligt underkända krav. Resultatet visar därmed att EN 18031 även fungerade som ett stöd för att identifiera vilka delar av produkten som kräver fortsatt utveckling innan full överensstämmelse kan uppnås.

Tabell 7. Sammanfattning av bedömda krav per modul

Tabell 7 sammanfattar hur de krav som ingick i den genomförda EN 18031-analysen fördelades per modul mellan Pass, Fail, Non-Conformity och N/A. Tabellen ger därmed en övergripande bild av vilka säkerhetsområden där produkten uppvisade uppfyllda krav, tydliga brister, kvarstående avvikelser respektive krav som inte bedömdes som tillämpliga.

Modul	Pass	Fail	Non-Conformity	N/A	Totalt
ACM	0	1	1	4	6
AUM	5	1	2	2	10
SUM	1	1	1	0	3
SSM	0	3	0	0	3
SCM	0	4	0	0	4
RLM	0	0	1	0	1
NMM	0	0	0	1	1
TCM	0	0	0	1	1
CCK	1	0	2	0	3
GEC	1	0	6	1	8
LGM	1	0	3	0	4
DLM	0	0	1	0	1
UNM	0	0	2	0	2
CRY	0	1	0	0	1
TOTALT	9	11	19	9	48

Värdena i tabellen anger antal krav per bedömningskategori inom respektive modul och utgör inte en poängskala eller riskskala. Tabellens syfte är att synliggöra hur den övergripande säkerhetsstatusen fördelade sig mellan olika moduler i EN 18031, snarare än att värdera enskilda kravs relativa vikt. Kategorin N/A avser krav som bedömdes som inte tillämpliga för den analyserade produkten.

Figur 4. Visuell översikt över bedömningsutfall per krav och modul i EN 18031 analysen.

För att komplettera den numeriska sammanställningen i Tabell 7 visas i Figur 4 en visuell översikt över hur de bedömda kraven fördelade sig inom den genomförda EN 18031-analysen. Figuren bygger på det använda bedömningsverktyget och sammanfattar bedömningsutfallet för respektive krav i de tre delar av standarden som var relevanta för den analyserade produkten.

Status on each Requirement for EN 18031-1												
ACM-1	ACM-2	AUM-1-1	AUM-1-2	AUM-2-1	AUM-3	AUM-4	AUM-5-1	AUM-5-2	AUM-6	SUM-1	SUM-2	SUM-3
Fail	Non-Conformity	Fail	Pass	Pass	Pass	Non-Conformity	Pass	Pass	Non-Conformity	Pass	Fail	Non-Conformity
SSM-1	SSM-2	SSM-3	SCM-1	SCM-2	SCM-3	SCM-4	RUM-1	NMM-1	TCM-1	CCK-1	CCK-2	CCK-3
Fail	Fail	Fail	Fail	Fail	Fail	Fail	Non-Conformity	N/A	N/A	Pass	Non-Conformity	Non-Conformity
GEC-1	GEC-2	GEC-3	GEC-4	GEC-5	GEC-6	CRY-1						
Non-Conformity	N/A	Non-Conformity	Non-Conformity	Pass	Non-Conformity	Fail						
Status on each Requirement for EN 18031-2												
ACM-3	ACM-4	ACM-5	ACM-6	AUM-2-2	LGM-1	LGM-2	LGM-3	LGM-4	DLM-1	UNM-1	UNM-2	GEC-7
N/A	N/A	N/A	N/A	N/A	Non-Conformity	Pass	Non-Conformity	Non-Conformity	Non-Conformity	Non-Conformity	Non-Conformity	Non-Conformity
Status on each Requirement for EN 18031-3												
AUM-1-3	GEC-8											
N/A	Non-Conformity											

Figuren gör det möjligt att överblicka hur bedömningarna fördelade sig mellan standardens tre delar och visar samtidigt vilka kravområden som främst präglades av uppfyllda krav, tydliga brister, kvarstående avvikelser respektive icke tillämpliga krav.

4.3 Identifierade risker

Analysen visar att enheten uppfyller flera grundläggande krav inom autentisering, lösenordsunikhet, uppdateringsmekanismens existens och intern logglagring. Samtidigt identifierades flera säkerhetsrisker kopplade till krav som bedömts som Fail eller Non-Conformity i EN 18031-analysen. Riskerna nedan beskriver hur dessa brister kan påverka produktens säkerhet i dess nuvarande utformning. För varje risk anges en bedömning av sannolikhet och konsekvens.

Okrypterad kommunikation (SCM-1, SCM-2, SCM-3, SCM-4 — Fail): Kommunikation mellan enheten och externa tjänster saknar tillräckligt skydd i samtliga kommunikationsflöden.

Sannolikhet: Hög — attackvektorn är nätverksåtkomlig, kräver ingen fysisk närvaro och inga autentiseringsuppgifter för att avlyssna trafik. *Konsekvens: Hög* — avlyssning kan exponera finansiella transaktionsdata, autentiseringsuppgifter och styrkommandon, vilket kan påverka både enskilda användare och operatören ekonomiskt.

Brister i uppdateringsmekanismen (SUM-2 — Fail): Avsaknad av tillräckligt skydd vid OTA-uppdateringar medför risk för att manipulerad eller obehörig programvara installeras på enheten.

Sannolikhet: Medelhög — attacken kräver tillgång till kommunikationskanalen men ingen fysisk åtkomst till enheten. *Konsekvens: Kritisk* — en komprometterad firmware ger angriparen full kontroll över enhetens funktioner och kan användas som plattform för vidare attacker mot nätverksinfrastruktur.

Otillräckligt skyddad intern lagring (SSM-1, SSM-2, SSM-3 — Fail): Känsliga data i enhetens interna minne riskerar att kunna extraheras eller missbrukas. *Sannolikhet: Medelhög* — kräver fysisk åtkomst till enheten, vilket begränsar attackytan men inte eliminerar risken i kommersiella installationer med många aktörer. *Konsekvens: Hög* — autentiseringsuppgifter och konfigurationsdata kan extraheras och användas för obehörig åtkomst till enhetens styrsystem eller molntjänster.

Brister i autentiseringsmekanismen (AUM-1-1 — Fail; AUM-4, AUM-6 — Non-Conformity): Otillräckligt skydd i autentiseringsrelaterade funktioner kan möjliggöra obehörig åtkomst.

Sannolikhet: Hög — brute force-attacker via nätverksgränssnitt förhindras inte aktivt eftersom skydd mot upprepade inloggningsförsök saknas. *Konsekvens: Hög* — obehörig åtkomst till enhetens styrsystem kan möjliggöra manipulation av laddningsfunktioner och exponering av användardata.

Begränsad loggning (LGM-1, LGM-3, LGM-4 — Non-Conformity): Otillräcklig loggning av säkerhetsincidenter försvårar spårbarhet och incidentutredning. *Sannolikhet: Låg* — bristen utnyttjas inte direkt som attackvektor utan ökar konsekvensen av andra angrepp. *Konsekvens: Medelhög* — avsaknad av loggdata försvårar forensisk analys och kan fördröja upptäckt och hantering av säkerhetsincidenter avsevärt.

Avsaknad av säker återställningsmekanism (DLM-1 — Non-Conformity): Känsliga data kan inte raderas kontrollerat vid avveckling eller ägarbyte. *Sannolikhet: Medelhög* — risken realiserar vid varje ägarbyte eller kassering av enheten, vilket är förväntat i en kommersiell driftsmiljö.

Konsekvens: Hög — tidigare användares autentiseringsuppgifter och energidata kan bli tillgängliga för ny ägare eller obehörig part.

Avsaknad av motståndskraft mot nätverksattacker (RLM-1 — Non-Conformity): Begränsat skydd mot nätverksbaserade störningar kan påverka enhetens tillgänglighet. *Sannolikhet: Medelhög* — internetexponerade enheter är regelbundet utsatta för automatiserade attacker och skanning.

Konsekvens: Hög — en lyckad överbelastningsattack kan slå ut laddningsfunktionen och påverka både användare och operatör ekonomiskt.

4.4 Förbättringsförslag

Baserat på de identifierade bristerna rekommenderas följande åtgärder för att förbättra enhetens säkerhetsstatus och uppfylla EN 18031:s krav:

All kommunikation mellan EV-laddaren och molntjänster bör krypteras med TLS 1.2 eller högre. Detta gäller både OCPP- och MQTT-protokollen som används för laddningshantering och fjärrstyrning. TLS säkerställer att data inte kan avlyssnas eller manipuleras under överföring.

OTA-uppdateringsprocessen bör kompletteras med krypterad överföring via HTTPS samt verifiering av firmware-filens äkthet med digital signatur innan installation. Detta förhindrar att manipulerad programvara installeras på enheten.

Känsliga data som lagras i enhetens interna minne bör skyddas med kryptering, exempelvis AES-128 eller AES-256. Detta skyddar autentiseringsuppgifter och annan känslig information mot obehörig åtkomst vid fysisk åtkomst till enheten.

Autentiseringsmekanismerna bör förstärkas med skydd mot upprepade inloggningsförsök, exempelvis genom kontolåsning eller fördröjning efter ett antal misslyckade försök. Lösenord bör genereras med en kryptografiskt säker slumpgenerator istället för deterministiska metoder. Möjlighet att uppdatera autentiseringsuppgifter på distans bör implementeras utan att kräva fysisk åtkomst till enheten.

5. Diskussion

Syftet med detta arbete var att undersöka hur EN 18031 kan användas som ett strukturerat ramverk för säkerhetsanalys av en IoT-enhet i en praktisk kontext. Diskussionen nedan tolkar resultaten och besvarar arbetets frågeställningar utan att upprepa dem.

EN 18031 som praktiskt analysverktyg:

Resultaten visar att EN 18031 fungerade väl som ett praktiskt analysverktyg. Det som gör standarden effektiv är dess moduluppbyggnad och beslutsträdstruktur, som tvingar fram konkreta frågor om varje säkerhetsområde och säkerställer att ingen aspekt förbises. Detta är särskilt värdefullt för tillverkare som saknar tidigare erfarenhet av strukturerad säkerhetsanalys, eftersom standarden erbjuder en tydlig och reproducerbar metod utan att kräva djup säkerhetsexpertis.

Det faktum att analysen identifierade brister inom flera moduler är inte förvånande. Forskning inom IoT-säkerhet visar att återkommande säkerhetsbrister är vanliga i uppkopplade produkter, och resultaten från detta arbete bekräftar det mönstret. Det intressanta är inte att bristerna existerar, utan att EN 18031 gjorde det möjligt att systematiskt identifiera och dokumentera dem på ett strukturerat sätt - något som utan ett sådant ramverk hade varit svårt att uppnå.

Varför krävdes samarbete med tillverkaren:

En verklig observation är att flera krav inte kunde bedömas enbart utifrån externt tillgänglig information. För att kunna göra korrekta bedömningar krävdes specifika frågor till tillverkaren om enhetens tekniska implementation. Detta säger något viktigt om hur EN 18031 bör användas i praktiken – standarden förutsätter ett nära samarbete mellan utvärderare och tillverkare och lämpar sig inte för extern granskning utan tillgång till intern teknisk dokumentation. För tillverkare som vill använda standarden som förberedelse inför CRA är detta en styrka snarare än en svaghet, eftersom det driver fram intern dokumentation och teknisk transparens.

Standarden mognad och tolkningssvårigheter:

EN 18031 är en relativt ny standard och kunskapen om hur vissa krav ska tolkas i praktiken är fortfarande begränsad. Under analysarbetet uppstod situationer där standardens beslutsträd lämnade utrymme för tolkning, vilket innebär att två utvärderare potentiellt kan komma fram till olika bedömningar för samma krav. Detta är en svaghet i standardens nuvarande form och något som kan förväntas förbättras i takt med att flera organisationer tillämpar den och vägledningsdokument utvecklas.

Studiens begränsningar:

Studien har flera begränsningar som påverkar dess trovärdighet och generaliserbarhet. Analysen baserades på en enskild IoT-enhet i samarbete med ett företag, vilket innebär resultaten inte kan generaliseras till andra produkttyper eller branscher. Konfidentialitetskravet innebär dessutom att analysen inte kan verifieras fullt ut externt, vilket begränsar arbetets vetenskapliga reproducerbarhet. Analysen var av analytisk karaktär och inkluderade inte praktisk teknisk testning eller verifiering av säkerhetslösningar, vilket innebär att vissa bedömningar baserades på tillgänglig dokumentation snarare än faktisk verifiering.

De sårbarhetsmönster som identifierades i denna studie — okrypterad kommunikation, bristande uppdateringsmekanismer, svag lagringssäkerhet och otillräcklig autentisering — stämmer väl överens med vad som dokumenterats i den bredare IoT-säkerhetslitteraturen. Sebestyen et al. [10] och Sadhu et al. [9] visar att dessa brister är återkommande och strukturella i IoT-produkter generellt, vilket stärker studiens externa validitet trots att den är avgränsad till en enskild enhet. De specifika riskerna mot OCPP-protokollet som identifierades i SCM-modulen bekräftar vidare de hot som Alcaraz et al. [15] dokumenterat för EV-laddinfrastruktur, och de autentiseringsbrister som framkom i AUM-modulen speglar det mönster som Luo et al. [11] och Neshenko et al. [12] beskriver som en av de svagaste länkarna i IoT-säkerhetsarkitekturer.

Implikationer för tillverkare inför CRA:

Resultaten indikerar att EN 18031 kan fungera som ett konkret förberedelsesteg inför CRA:s ikraftträdande 2027. En tidig analys ger tillverkare en tydlig bild av var deras produkt står i förhållande till standardens krav och vilka åtgärder som behöver vidtas. Det är dock viktigt att poängtera att EN 18031-analys inte är detsamma som CRA-efterlevnad – standarden adresserar de tekniska kraven men CRA ställer även krav på processer, dokumentation och livscykelhantering som går utöver vad en enskild produktanalys kan täcka.

6. Slutsats

Syftet med detta arbete var att undersöka hur EN 18031 kan användas som ett strukturerat ramverk för säkerhetsanalys av en IoT-enhet i en praktisk kontext. Arbetet genomfördes som fallstudie i samarbete med iThing AB, där en verklig EV-laddare analyserades med EN 18031 som ramverk.

Resultaten visar att EN 18031 fungerar som ett praktiskt och användbart analysverktyg för IoT-enheter. Standardens moduluppbyggnad och beslutsträdsstruktur möjliggjorde en systematisk och reproducerbar säkerhetsanalys som identifierade brister inom flera säkerhetsområden. Analysen bekräftar att EN 18031 inte bara är ett teoretiskt ramverk utan ett konkret verktyg som tillverkare kan använda för att strukturera sitt säkerhetsarbete.

Sammanfattningsvis besvarar arbetet sina tre frågeställningar: EN 18031 ställer tydliga och strukturerade krav på IoT-enheters säkerhet, standarden kan tillämpas praktiskt på en verklig IoT-enhet genom ett systematiskt analysarbete i samarbete med tillverkaren, och en EN 18031-baserad analys utgör ett konkret och genomförbart förberedelsesteg inför CRA.

Det bör dock noteras att resultaten i detta arbete baseras på en enskild enhet från ett specifikt företag och därmed inte kan generaliseras till andra IoT-produkter eller branscher. Varje produkt har sin unika tekniska implementation och säkerhetsprofil, vilket innebär att liknande analyser av andra enheter kan ge väsentligt annorlunda resultat. Vidare genomfördes ingen praktisk penetrationstestning för att verifiera de identifierade bristerna, vilket innebär att analysens slutsatser bygger på dokumentationsgranskning och tillverkarens uppgifter snarare än faktisk teknisk verifiering.

7. Framtida arbete

Detta arbete har undersökt hur EN 18031 kan tillämpas på en enskild IoT-enhet i en specifik kontext. För att bredda och fördjupa kunskapen inom området föreslås följande riktningar för framtida arbete.

En naturlig fortsättning är att tillämpa EN 18031 på fler IoT-enhetstyper inom olika branscher, exempelvis medicinsk utrustning, industriell automation eller smarta hemanheter. En sådan jämförelse skulle ge en bredare bild av standardens tillämpbarhet och synliggöra om vissa enhetstyper uppvisar specifika säkerhetsmönster.

En djupare teknisk analys av den analyserade enheten, där bedömningar verifieras genom praktisk säkerhetstestning snarare än enbart dokumentationsgranskning, skulle stärka analysens trovärdighet och ge en mer fullständig bild av enhetens faktiska säkerhetsstatus.

Det vore också värdefullt att studera hur ett verkligt CRA-efterlevnadsarbete ser ut i praktiken - från EN 18031-analys till faktisk certifiering. Ett sådant arbete skulle belysa gapet mellan en strukturerad säkerhetsanalys och full regulatorisk efterlevnad.

Slutligen skulle det vara intressant att undersöka hur EN 18031 kan integreras tidigare i produktutvecklingsprocessen, exempelvis som en del av ett säkert utvecklingsramverk. En tidig integration av standardens krav i designfasen skulle potentiellt minska kostnaderna för att åtgärda säkerhetsbrister jämfört med att genomföra analysen efter att produkten är färdigutvecklad.

Därutöver skulle det vara värdefullt om en uppföljande studie tillämpar en fullständig TARAanalys på samma EV-laddare, för att komplettera EN 18031-resultaten med strukturerad hotmodellering och formell riskpoängsättning.

8. Referenser

- [1] NIST, *Establishing IoT Device Cybersecurity Requirements*. Hämtad 29 mars 2026 från <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213.pdf>
- [2] CENELEC, *New Cybersecurity Standards Support Compliance with RED Directive*. Hämtad 29 mars 2026 från <https://www.cenelec.eu/news-events/news/2025/newsletter/ots-59-cybersecurity-standards/>.
- [3] European Commission, *Cyber Resilience Act*. Hämtad 19 mars 2026 från <https://digitalstrategy.ec.europa.eu/en/policies/cyber-resilience-act>
- [4] NIST, *IoT Device Cybersecurity Requirement Catalog*. Hämtad 29 mars 2026 från <https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-213A.pdf>
- [5] ENISA, *The IoT Security Gap*. Hämtad 19 mars 2026 från <https://www.enisa.europa.eu/sites/default/files/publications/WP2018%20O.1.3.1%20IoT%20standards.pdf>
- [6] Nemko, *The harmonized standard*. Hämtad 19 mars 2026 från <https://www.nemko.com/hubfs/2025-02-25%20Webinar%20-%20for%20distribution.pdf>
- [7] NIST, *Considerations for Managing Internet of Things (IoT) Cybersecurity and Privacy*

- Risk. Hämtad 19 mars 2026 från <https://nvlpubs.nist.gov/nistpubs/ir/2019/nist.ir.8228.pdf>
- [8] European Commission, *Commission Delegated Regulation (EU) 2022/30 supplementing Directive 2014/53/EU — cybersecurity requirements for radio equipment*. Official Journal of the European Union. Hämtad 19 mars 2026 från <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32022R0030>
- [9] MDPI Sensors, *Internet of Things: Security and Solutions Survey*. Hämtad 25 mars 2026 från <https://www.mdpi.com/1424-8220/22/19/7433>
- [10] Sebestyen, H., Popescu, D. E., & Zmaranda, R. D. *A Literature Review on Security in the Internet of Things: Identifying and Analysing Critical Categories*. *Computers*, 14(2), 61. Hämtad 25 mars 2026 från <https://www.mdpi.com/2073-431X/14/2/61>.
- [11] ACM Computing Surveys, *IoT Authentication Protocols: Challenges, and Comparative Analysis*. Hämtad 25 mars 2026 från <https://dl.acm.org/doi/10.1145/3703444>
- [12] ACM Computing Surveys, *A Systematic Review of IoT Security: Research Potential, Challenges, and Future Directions*. Hämtad 25 mars 2026 från <https://dl.acm.org/doi/10.1145/3625094>
- [13] Springer, *Implementation of SSL/TLS Security with MQTT Protocol in IoT Environment*. Hämtad 25 mars 2026 från <https://link.springer.com/article/10.1007/s11277-023-10605-y>
- [14] MDPI Energies, *Johnson, J.; Berg, T.; Anderson, B.; Wright, B., Review of Electric Vehicle Charger Cybersecurity Vulnerabilities, Potential Impacts, and Defenses*. Hämtad 25 mars 2026 från <https://www.mdpi.com/1996-1073/15/11/3931>
- [15] Springer, *OCCP in the spotlight: threats and countermeasures for electric vehicle charging infrastructures 4.0*. Hämtad 25 mars 2026 från <https://link.springer.com/article/10.1007/s10207-023-00698-8>
- [16] Springer, *The EU's cybersecurity framework: the interplay between the Cyber Resilience Act and the NIS 2 Directive*. Hämtad 25 mars 2026 från <https://link.springer.com/article/10.1365/s43439-023-00084-z>
- [17] NIST, *Foundational Cybersecurity Activities for IoT Device Manufacturers*. Hämtad 25 mars 2026 från <https://nvlpubs.nist.gov/nistpubs/ir/2020/NIST.IR.8259.pdf>
- [18] International Organization for Standardization, *ISO/SAE 21434:2021 Road vehicles — Cybersecurity engineering*. Hämtad 25 mars 2026 från <https://www.iso.org/standard/70918.html>
- [19] NIST. (2012). *SP 800-30 Rev. 1: Guide for Conducting Risk Assessments*. National Institute of Standards and Technology. Hämtad 25 april 2026 från <https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-30r1.pdf>.

9. Bilagor

Bilaga 1. Sammanställning av bedömda krav

Tabellen nedan sammanställer samtliga 48 bedömda krav från EN 18031-analysen. Kraven är uppdelade per bedömningskategori för att underlätta läsbarhet och överblick.

Bilaga 1a. Uppfyllda krav (Pass) – 9 krav

Modul	Krav-ID	Motivering
AUM	AUM 1–2	Åtkomst via användargränssnitt kräver autentisering med användarnamn och lösenord
AUM	AUM 2–1	Minst en autentiseringsfaktor används — lösenord utgör kunskapsfaktor
AUM	AUM-3	Autentisering valideras serversidan för samtliga kommunikationsmekanismer
AUM	AUM 5–1	Lösenord är unikt per enhet
AUM	AUM 5–2	Lösenord provisionerat av auktoriserad tillverkare vid tillverkning
SUM	SUM-1	Uppdateringsmekanismen finns implementerad
CCK	CCK-1	WiFi WPA2 använder AES-128 som uppfyller minimikravet på 112-bitars säkerhetsstyrka
GEC	GEC-5	Fysiskt gränssnitt är nödvändigt för enhetens avsedda funktion
LGM	LGM-2	Loggdata lagras i persistent intern lagring som behåller data vid omstart

Bilaga 1b. Underkända krav (Fail) — 11 krav

Dessa krav bedömdes som ej uppfyllda eftersom analysen visade tydliga brister i produktens nuvarande utformning. Varje Fail representerar ett identifierat säkerhetsgap som kräver åtgärd.

Modul	Krav-ID	Motivering
ACM	ACM-1	Åtkomstkontroll saknas för firmware och NVS-Flash i produktens nuvarande utformning
AUM	AUM 1-1	Verifiering av identiteten hos anslutande användare och system uppfyller inte kravet
SUM	SUM-2	OTA-uppdateringen saknar tillräckligt skydd mot installation av manipulerad firmware
SSM	SSM-1	Skydd av känsliga data i intern lagring uppfyller inte standardens krav
SSM	SSM-2	Integritetsskydd för lagrade säkerhetsparametrar är inte tillräckligt implementerat
SSM	SSM-3	Konfidentialitetsskydd för känsliga konfigurationsdata uppfyller inte kravet
SCM	SCM-1	OCPK-kommunikation saknar bekräftad TLS-kryptering
SCM	SCM-2	MQTT-kommunikation saknar bekräftad TLS-kryptering
SCM	SCM-3	Autentisering av kommunikationspart uppfyller inte kravet för extern kommunikation

SCM	SCM-4	Skydd mot trafikmanipulation under överföring är inte tillräckligt implementerat
CRY	CRY-1	Kryptografianvändningen uppfyller inte kravet på bästa praxis fullt ut

Bilaga 1c. Krav med avvikelse (Non-Conformity) — 19 krav

Dessa krav kunde inte bedömas som uppfyllda i produktens nuvarande utformning, men bristen är inte definitiv. Implementationen är antingen påbörjad men inte färdigställd, eller så saknas dokumentation som krävs för ett Pass.

Modul	Krav-ID	Motivering
ACM	ACM-2	Åtkomstkontroll till skyddade resurser är inte färdigimplementerad — mekanismen finns delvis men saknar fullständig täckning
AUM	AUM-4	Skydd mot upprepade inloggningsförsök saknas i nuvarande utformning
AUM	AUM-6	Uppdatering av autentiseringsuppgifter på distans är inte implementerad
SUM	SUM-3	Verifiering av uppdateringsprocessens integritet är inte färdigställd
RLM	RLM-1	Motståndskraft mot nätverksbaserade störningar är inte implementerad
CCK	CCK-2	Kryptografiskt säker nyckelgenerering kan inte bekräftas
CCK	CCK-3	Nyckelhantering och livscykelkydd för kryptografiska nycklar är inte färdigimplementerat
GEC	GEC-1	Sårbarhetsbedömning av ingående komponenter är inte dokumenterad i tillräcklig omfattning
GEC	GEC-3	Inputvalidering för data via nätverksgränssnitt är inte bekräftat implementerat

GEC	GEC-4	Säker hantering av felfall och undantagstillstånd är inte fullt dokumenterad
GEC	GEC-6	Minimering av attackyta genom avaktivering av oanvända tjänster kan inte bekräftas
GEC	GEC-7	Säker programvaruutvecklingsprocess är inte dokumenterat uppfyllt
GEC	GEC-8	Hantering av tredjepartskomponenter och deras säkerhetsstatus är inte dokumenterad
LGM	LGM-1	Loggning av autentiseringshändelser är inte bekräftat implementerad i tillräcklig omfattning
LGM	LGM-3	Skydd av loggdata mot obehörig manipulering är inte bekräftat implementerat
LGM	LGM-4	Exportmöjlighet för loggdata för incidentutredning är inte implementerad
DLM	DLM-1	Säker radering av persondata vid avveckling eller ägarbyte är inte implementerad
UNM	UNM-1	Användarinformation om datainsamling är inte implementerad i produktens nuvarande utformning
UNM	UNM-2	Mekanism för användarens samtycke till datainsamling saknas

Bilaga 1d. Ej tillämpliga krav (N/A) — 9 krav

Dessa krav bedömdes som inte tillämpliga för den analyserade produkten baserat på dess faktiska funktioner, gränssnitt och användningskontext. De ingår inte i den detaljerade analysen.

Modul	Krav-ID	Motivering
ACM	ACM-3	Kravet avser åtkomstkontroll för lokala nätverkstjänster och administrativa gränssnitt som inte är aktiva i den analyserade produktkonfigurationen
ACM	ACM-4	Kravet avser åtkomstkontroll för externa API-anslutningar från tredjepartstjänster, vilket inte är tillämpligt eftersom enheten inte exponerar ett externt API i sin nuvarande utformning
ACM	ACM-5	Kravet avser rollbaserad behörighetsstyrning med flera användarnivåer, vilket inte är implementerat i enhetens arkitektur då den endast hanterar en enda operatörsroll
ACM	ACM-6	Kravet avser tidsbegränsad sessionshantering för interaktiva användarsessioner, vilket inte är tillämpligt för denna enhetstyp då enheten saknar ett sessionbaserat användargränssnitt
AUM	AUM-2-2	Kravet avser autentiseringsmetoder som inte är tillämpliga för denna produktkonfiguration
AUM	AUM-1-3	Kravet avser autentiseringsscenarier som inte är tillämpliga för denna produkt
NMM	NMM-1	Nätverksövervakningsmekanismer bedömdes som inte tillämpliga för denna produkttyp
TCM	TCM-1	Trafikstyrningsmekanismer bedömdes som inte tillämpliga för denna produkttyp
GEC	GEC-2	Kravet avser funktioner som inte används av den analyserade produkten

Bilaga 2. Tillgångsregister

Hoten per tillgång identifierades baserat på tre källor: (1) EN 18031-analysens Failutfall, som direkt pekar på vilka skyddsmekanismer som saknas för respektive tillgång; (2) befintlig forskning om IoT-sårbarhetsmönster (se avsnitt 2.5, särskilt Alcaraz et al. [15] och Wright [14]); samt (3) teknisk dialog med tillverkaren om enhetens kommunikationsflöden och lagringsarkitektur. Ingen aktiv exploit-testning genomfördes.

Tillgång	Typ	Beskrivning	EN 18031moduler	Potentiella hot
Start/Stoppladdning	Säkerhetstillgång	Styrfunktion som aktiverar och avaktiverar laddning	ACM, AUM, RLM	Obehörig aktivering eller avaktivering av laddning
Fordonskommunikation	Nätverkstillgång	Kommunikation med fordonet via PWM-signal	GEC, SCM	Manipulation av laddningssignal
Firmware	Säkerhetstillgång	Enhetens programvara som styr all funktionalitet	SUM, GEC	Installation av manipulerad firmware via OTA
NVS-Flash	Säkerhetstillgång	Internt lagringsutrymme för känsliga konfigurationsdata och autentiseringsuppgifter	SSM, CCK	Extraktion av känsliga data vid fysisk åtkomst
Autentiseringsuppgifter	Säkerhetstillgång	Användarnamn och lösenord för åtkomst till enhetens funktioner	AUM, CCK	Brute force-attacker, obehörig åtkomst
Lösenord	Säkerhetstillgång	Enhetsunika lösenord provisionerade vid tillverkning	AUM, CCK	Avlyssning eller extraktion av lösenord
OCPP 1.6	Nätverkstillgång	Kommunikationsprotokoll mellan laddaren och molnbackend	SCM, ACM	Avlyssning, man-in-the-middle-attack
MQTT	Nätverkstillgång	Meddelandeprotokoll för fjärrstyrning och dataöverföring	SCM, ACM	Avlyssning, obehörig publicering av meddelanden
Interna energidata	Finansiell tillgång	Energiförbrukningsdata kopplad till finansiella transaktioner	SCM, UNM, DLM	Manipulering av faktureringsdata, dataintrång

Bilaga 3. Mappning av tillgångar till hot och attackvektorer

Attackvektorerna i tabellen nedan är härledda ur EN 18031-analysens Fail-utfall — varje Fail identifierar vilken kommunikationskanal, lagringskomponent eller mekanism som saknar skydd, vilket direkt anger den potentiella attackvektorn. Vektorerna kompletterades med kända attackmetoder för EV-laddare och IoT-kommunikation från litteraturen. Ingen praktisk verifiering av vektorerna genomfördes.

Tillgång	Hot	Attackvektor
Start/Stoppladdning	Obehörig aktivering eller avaktivering av laddningsfunktion	Nätverksbaserad attack via OCPP eller MQTT utan autentisering
Fordonskommunikation	Manipulation av PWM-signal som styr laddningseffekt	Fysisk åtkomst till enhetens gränssnitt
Firmware	Installation av manipulerad firmware som ger angriparen kontroll över enheten	OTA-uppdateringskanal utan signaturverifiering
NVS-Flash	Extraktion av autentiseringsuppgifter och konfigurationsdata	Fysisk åtkomst till enheten utan krypteringsskydd
Autentiseringsuppgifter	Obehörig åtkomst till enhetens styrsystem via brute force	Nätverksbaserad attack mot autentiseringsgränssnitt utan skydd mot upprepade försök
Lösenord	Avlyssning av lösenord under överföring eller extraktion från minne	Okrypterad kommunikation eller fysisk åtkomst till NVS-Flash
OCPP 1.6	Avlyssning av kommunikation mellan laddare och molnbackend	Man-in-the-middleattack på okrypterad OCPP-trafik
MQTT	Obehörig publicering av meddelanden som manipulerar enhetens beteende	Nätverksbaserad attack mot MQTT-broker utan tillräcklig åtkomstkontroll
Interna energidata	Manipulering av energidata som påverkar fakturering	Obehörig åtkomst via nätverksgränssnitt eller avlyssning av dataöverföring