https://doi.org/10.17559/JF-2026010000018

Zaprimljen: 10.7.2025.
Odobren za objavu: 27.1.2026.
Pregledni rad

# ANALIZA SIGURNOSNIH PRIJETNJI I MJERA ZAŠTITE U SUSTAVIMA DALJINSKOG OČITANJA BROJILA ELEKTRIČNE ENERGIJE

Maja Čuletić Čondrić[1], Silvio Vilagoš[2], Marijana Zarožinski[3]
[1] Sveučilište u Slavonskom Brodu, Trg I. B. Mažuranić 2, 35000 Slavonski Brod, Hrvatska,
[2] Sveučilište u Slavonskom Brodu, student
[3] Industrijsko-obrtnička škola, E. Kumičića 55, 35000 Slavonski Brod, Hrvatska
mccondric@unisb.hr

Sažetak: U ovom radu analiziraju se metode očitanja električne energije s posebnim naglaskom na sigurnosne aspekte i ekonomsku isplativost sustava daljinskog očitanja brojila. Rad obuhvaća usporedbu tradicionalnih metoda očitanja, samoočitanja korisnika i daljinskog očitanja kroz kriterije troškova, točnosti, učinkovitosti i sigurnosti podataka. Posebna pažnja posvećena je sigurnosnim rizicima daljinskog očitanja te mjerama zaštite od kibernetičkih napada i njihovoj ulozi u očuvanju povjerljivosti i integriteta podataka. Metodologija rada temelji se na pregledu relevantne literature i komparativnoj analizi isplativosti pojedinih metoda. Rezultati analize pokazuju da daljinsko očitanje, uz primjenu standardiziranih sigurnosnih mehanizama poput enkripcije i kontrole pristupa, pruža višu razinu sigurnosti i operativne učinkovitosti te predstavlja dugoročno održivo i pouzdano rješenje, unatoč većim početnim troškovima implementacije.

Ključne riječi: daljinsko očitanje, kibernetička sigurnost, ranjivosti, zaštita podataka.

## 1. Uvod

Rad se bavi analizom metoda očitanja električne energije u složenom okruženju s različitim zahtjevima i ograničenjima, s posebnim naglaskom na sigurnosne aspekte sustava daljinskog očitanja električnih brojila (Semlambo, Mfoi i Sangula, 2022). Očitanje potrošnje energije ključan je proces u funkcioniranju elektroenergetskog sustava (Momoh, 2008). Tradicionalne metode očitanja, poput ručnog očitavanja od strane operatera, postaju sve skuplje i neučinkovitije u modernom dobu, karakteriziranom rastućim brojem potrošača i sve većim zahtjevima za preciznošću i učestalošću mjerenja. Samoočitanje, iako jeftinije, često je podložno pogreškama i manipulacijama. Daljinsko očitanje, s druge strane, nudi potencijal za automatizaciju, povećanje točnosti i dostupnost podataka u stvarnom vremenu, ali postavlja i nove izazove vezane uz troškove implementacije, sigurnost podataka i integraciju s postojećim sustavima.

Kibernetička sigurnost je sustav organizacijskih i tehničkih mjera za zaštitu računalnih sustava, mreža i podataka od digitalnih napada, s ciljem osiguranja povjerljivosti, integriteta, autentičnosti i dostupnosti informacija (Kizza, 2017). Obuhvaća zaštitu od hakiranja, neovlaštenog pristupa, oštećenja podataka i prekida poslovnih procesa. Zaštita kritične infrastrukture predstavlja strateški prioritet jer se radi o sustavima ključnim za funkcioniranje društva, kao što su: energetika, transport, zdravstvo, telekomunikacije i

slično (Skok, 2002; Stojkov, Baus, Barukčić i Provči, 2015). Kibernetički napadi na te sustave mogu izazvati kaskadne posljedice po društveno-ekonomsku stabilnost. Pregled postojeće literature pokazuje da se većina istraživanja usmjerava na tehničke i organizacijske izazove daljinskog očitanja, dok je integrirani pristup koji

povezuje sigurnosne rizike, mjere zaštite i ekonomsku isplativost rjeđe zastupljen, što predstavlja temeljni cilj ovoga rada.

## 2. Metode očitanja energije

Odabir optimalne metode očitanja energije u složenom okruženju sa

različitim zahtjevima i ograničenjima predstavlja posebnu problematiku u kojoj je potrebno uzeti u obzir sve prednosti i nedostatke postojećih metoda očitanja energije kao što su očitanje operatera, samoočitanje korisnika, daljinsko očitanje, ali i njihove tehničke te ekonomske aspekte (Benzi F., Anglani N., Bassi E., Frosini L., 2011).

### 2.1. Očitanje od strane operatera

Očitanje od strane operatera uključuje slanje ovlaštenog djelatnika na lokaciju brojila radi ručnog očitanja potrošnje energije. Djelatnik vizualno pregledava brojilo i zapisuje očitanu vrijednost, koja se kasnije unosi u sustav za obradu podataka. Prednosti ove metode su: jednostavnost implementacije (ne zahtijeva naprednu tehnologiju), te mogućnost vizualne provjere stanja brojila. Dok su nedostaci poput visokih troškova rada, vremenski zahtjevno i neučinkovito, podložnost ljudskim pogreškama, te ograničena učestalost očitanja.

### 2.2. Samoočitanje korisnika

Samoočitanje korisnika omogućuje potrošačima da sami očitaju stanje brojila i dostave podatke energetskoj tvrtki. Korisnici obično dostavljaju podatke putem telefona, interneta ili slanjem obrasca. Prednosti ove metode su: niži troškovi u usporedbi s očitanjem od strane operatera, te veća uključenost korisnika. Dok su nedostaci: mogućnost netočnih očitanja (nenamjerne pogreške korisnika), kao i rizik od manipulacija (namjerno lažno prikazivanje potrošnje), ali i disciplina korisnika.

### 2.3. Daljinsko očitanje

Daljinsko očitanje (eng. Automatic Meter Reading - AMR) koristi tehnologiju za automatsko prikupljanje podataka o potrošnji energije s udaljenih lokacija, bez potrebe za ljudskom intervencijom na licu mjesta. Podaci se prenose komunikacijskim tehnologijama kao što su PLC (Power Line Communication), mobilne komunikacijske mreže te RF bežične mreže. Prednosti ove metode uključuju visoku točnost i pouzdanost, mogućnost čestog i redovitog očitanja, smanjeni troškovi rada, poboljšana učinkovitost i brzina prikupljanja podataka te podrška za napredne funkcionalnosti kao što su daljinsko uključivanje i/ili isključivanje, detekcija prekida u opskrbi i slično. Nedostaci također postoje, a oni su: visoki troškovi implementacije za infrastrukturu, i opremu, potencijalni problemi sa sigurnošću podataka, kao i ovisnost o pouzdanosti komunikacijske infrastrukture.

### 2.4. Usporedna analiza metoda očitanja i njihova isplativost

Sustavi očitavanja električnih brojila razvili su se kako bi odgovorili na potrebe za točnošću, ekonomičnošću i sigurnošću. U tablici 1 navedeni su kriteriji koji su se analizirali te njihove karakteristike za svaku spomenutu metodu.

Metodološki pristup rada temelji se na kvalitativnoj analizi literature i komparativnoj evaluaciji metoda očitanja električne energije. Sigurnosni aspekti procjenjivani su prema kriterijima

povjerljivosti, integriteta i dostupnosti podataka, dok su mjere zaštite analizirane s obzirom na njihovu ulogu u smanjenju rizika neovlaštenog pristupa, manipulacije podacima i narušavanja privatnosti korisnika.

Tablica 1. Usporedba kriterija metoda očitanja

| Kriterij | Očitanje od strane operatera | Samoočitanje korisnika | Daljinsko očitanje |
|---|---|---|---|
| Troškovi | Visoki | Niski | Visoki (početni), niski (dugoročni) |
| Točnost | Niska do srednja | Niska do srednja | Visoka |
| Efikasnost | Niska | Srednja | Visoka |
| Angažman korisnika | Nizak | Srednji | Različit (ovisi o implementaciji) |
| Sigurnost podataka | Srednja | Srednja | Visoka (uz odgovarajuće mjere) |
| Učestalost očitanja | Niska | Niska | Visoka |
| Dodatne funkcionalnosti | Nema | Nema | Moguće (npr. daljinsko upravljanje, detekcija kvara) |

Svaka metoda ima specifične troškovne implikacije, koje se analiziraju kroz strukturu naknada, operativne troškove i utjecaj na konačni račun korisnika (Majdandžić, 2004). Pri usporedbi troškova potrebno je razlikovati direktne naknade, odnosno one naknade koje se eksplicitno naplaćuju korisnicima, od indirektnih troškova tj. troškova uključenih u tarife ili operativne troškove sustava.

Troškovi se definiraju prema sljedeća tri kriterija, a to su:

1) Standardnom očitanju (redovito šestomjesečno očitanje bez dodatnih naknada),
2) Izvanrednom očitanju (na zahtjev korisnika, uz naknadu temeljenu na stvarnim troškovima),
3) Samoočitanju (besplatno za korisnike u režimu šestomjesečnog očitanja, uz obvezu mjesečne dostave podataka)

Kod metode samoočitanja sigurnost pohrane podataka nije primarni problem, budući da se podaci pohranjuju u sustav operatera, kao i u slučaju daljinskog očitanja. Međutim, razina sigurnosti ocijenjena je srednjom zbog povećanog rizika netočnog ili namjerno pogrešnog unosa podataka od strane korisnika, što utječe na pouzdanost sustava, ali ne i na sigurnost same pohrane podataka.

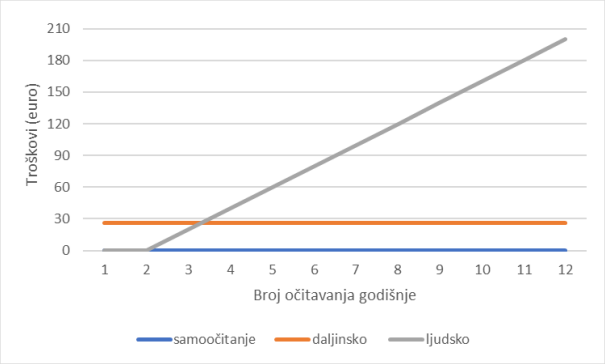
Na temelju prikupljenih podataka napravljena je komparativna analiza troškova koja je prikazana u Tablici 2., gdje je uočeno kako je troškovno najpovoljnija metoda za većinu kućanstava samoočitanje, pod uvjetom redovitog i točnog dostavljanja podataka. Daljinska očitanja nude tehnološku naprednost, ali su trenutno ekonomično opravdana samo u kontekstu šire modernizacije mreže. Za korisnike koji često izostaju s lokacije, izvanredna ljudska očitanja mogu postati skup izbor.

Tablica 2. Usporedba troškova metoda očitanja

| Metoda očitanja | Direktni troškovi za korisnika | Indirektni troškovi | Rizici dodatnih troškova |
|---|---|---|---|
| **Daljinsko** | 0 eura | Uključeno u tarifu (~ 14 eura/6 mj.) | Visoki početni ulozi sustava |

| | | | |
|---|---|---|---|
| **Ljudsko (standardno)** | 0 eura | Uključeno u tarifu | Kašnjenja u očitanju |
| **Ljudsko (izvanredno)** | ~ 20 eura/zahtjev | Nema | Ovisnost o raspoloživosti radnika |
| **Samoočitanje** | 0 eura | Uključeno u tarifu | Kažnjava se procijenjenim računima |

Posebno područje za daljnja razmatranja je utjecaj na točnost obračuna, ali može se reći da daljinsko očitanje osigurava vrlo visoku razinu točnosti, dok samoočitanje uvelike ovisi o disciplini korisnika. Procijenjeni obračuni kod kašnjenja u samoočitanju mogu dovesti do kumulativnih odstupanja od 10-15% tijekom šestomjesečnog ciklusa. Nakon prikupljenih podataka, grafičkim prikazom (Slika 1.) jasno se mogu identificirati prijelomne točke kada je pojedina metoda očitavanja električnih brojila financijski isplativija za krajnjeg korisnika. U ukupan trošak uzelo se u obzir ugradnja pametnog brojila kod daljinskog očitanja, zatim kod ljudskog izvanrednog očitanja vidljiv je linearni rast jer se naplaćuje po svakom pojedinom zahtjevu, dok je samoočitanje za korisnika besplatno pod uvjetom da se podaci dostavljaju na vrijeme i točno.




Slika 1: Isplativost metoda očitavanja električnih brojila

Prijelomna točka, odnosno trenutak kada ljudsko očitanje postaje skuplje od daljinskog ili samoočitanja, događa se već kod trećeg očitanja godišnje. Samoočitanje i daljinsko očitanje ostaju na konstantno niskoj razini, dok trošak ljudskog očitanja eksponencijalno raste s povećanjem broja očitavanja (Pejić Bach i sur., 2016).

## 3. Sigurnost i zaštita daljinskog očitanja

Svaka metoda očitanja električnih brojila nosi specifične sigurnosne rizike koji mogu utjecati na potrošače, distributere električne energije i širu energetsku infrastrukturu (Luring, Szameitat, Hoffmann i Bumiller, 2018). Sigurnost daljinskog očitanja brojila za struju za kućanstva temelji se na nekoliko ključnih aspekata, kao što su: tehnička sigurnost i zaštita podataka, prednosti za korisnike i isporučitelje, kao i kibernetički rizici i izazovi.

### 3.1. Sigurnost daljinskog očitanja brojila za struju za kućanstva

Tehnička sigurnost i zaštita podataka uvelike doprinosi sigurnosti daljinskog očitanja brojila za struju u kućanstvu. Dakle, pametna brojila koriste napredne metode enkripcije za zaštitu prijenosa podataka između brojila i centralnog sustava, čime se sprječava neovlašteni pristup i manipulacija podacima. Zatim, svaki pokušaj neovlaštenog pristupa ili izmijene očitanja automatski aktivira alarmni sustav, čime se učinkovito sprječava krađa električne energije i neovlašteno korištenje podataka. Prijenos podataka je zaštićen komunikacijskim i prijenosnim protokolima, a pristup podacima imaju samo stručno osposobljene osobe. Isporučitelji električne energije mogu bolje upravljati mrežom, brže otkrivati gubitke i optimizirati potrošnju, a korisnicima je omogućeno lakše upravljanje vlastitom potrošnjom jer dobivaju pravovremene obavijesti o povećanoj potrošnji ili mogućim kvarovima, što omogućuje brzu reakciju i smanjuje rizik. Također, pametna brojila predstavljaju potencijalne ulazne

točke za kibernetičke napade jer su dio šire mreže uređaja (IoT) te napadači mogu pokušati iskoristiti ranjivosti u brojilima za pristup širem sustavu, što može ugroziti ne samo pojedinačna kućanstva, već i širu energetsku infrastrukturu.

### 3.2. Sigurnosni rizici kod daljinskog očitanja brojila

Za analizu sigurnosnih rizika ključno je razumijevanje cjelokupne isplativosti i održivosti pojedinih sustava očitanja, pa tako i daljinskog očitanja brojila. Pametna brojila su upravo glavna meta za kibernetičke napade i njihove sigurnosne rizike. Kada se govori o rizicima digitalnog pristupa tu se ubrajaju neovlašteni pristupi i hakiranje, manjkava enkripcija i nedostatak autentifikacije. Uspješan napad na jedno brojilo može potencijalno omogućiti pristup široj mreži ili drugim povezanim uređajima u kućanstvu, napadači mogu manipulirati očitanjima brojila kako bi prikazali manju i/ili veću potrošnju, te sve to dovodi do ranjivosti infrastrukture i sistemskih rizika koji su neizostavni. Također, postoje rizici za privatnost podataka gdje su u fokusu detaljni obrasci potrošnje koje pametna brojila prikupljaju, kao i njihova potencijalna zloupotreba tj. krađa identiteta, praćenje prisutnosti ukućana i slično (Bača, 2004).

### 3.3. Zaštita daljinskog očitanja brojila od kibernetičkih napada

Daljinsko očitanje brojila za struju za kućanstva štiti se od kibernetičkih napada primjenom više slojeva sigurnosnih mjera, koje uključuju:

a) višefaktorska autentifikacija (MFA),
b) kontrola pristupa,
c) redovito ažuriranje i zakrpe,
d) kriptografska zaštita,
e) antivirusna zaštita i vatrozidi,
f) smanjenje površine napada,
g) edukacija korisnika i zaposlenika,
h) sigurnosne kopije.

Višefaktorska autentifikacija značajno smanjuje rizik neovlaštenog pristupa jer zahtijeva kombinaciju više neovisnih faktora, čime se kompromitacija jedne vjerodajnice ne smatra dovoljnom za pristup sustavu. Kriptografska zaštita prijenosa podataka sprječava presretanje i izmjenu podataka tijekom komunikacije između brojila i centralnog sustava. Redovito ažuriranje sustava i primjena sigurnosnih zakrpa ključno su za uklanjanje poznatih ranjivosti koje napadači mogu iskoristiti. Edukacija korisnika i zaposlenika dodatno smanjuje rizik socijalnog inženjeringa, koji je jedan od najčešćih vektora napada.

Ove mjere zajedno čine robustan sigurnosni okvir koji štiti sustave daljinskog očitanja brojila od najčešćih kibernetičkih prijetnji, uključujući neovlašteni pristup, krađu podataka i sabotažu infrastrukture (Kim i Solomon, 2018). Evaluacija sigurnosnih mjera provedena je kvalitativno, kroz usporedbu njihove učinkovitosti u sprječavanju najčešćih kibernetičkih prijetnji, pri čemu je naglasak stavljen na njihovu primjenjivost u stvarnim sustavima daljinskog očitanja. Sigurnosni pristupi opisani u ovom radu usklađeni su s preporukama za zaštitu napredne mjerne infrastrukture u pametnim mrežama, kako ih navode novija istraživanja iz područja kibernetičke sigurnosti pametnih mreža (Gungor et al., 2019).

### 3.4. Standardi za implementaciju daljinskog očitanja

Sustavi daljinskog očitanja električne energije temelje se na međunarodno prihvaćenim standardima koji osiguravaju interoperabilnost, sigurnost i pouzdanost komunikacije. Najčešće korišten standard u Europi je DLMS/COSEM (IEC 62056), koji definira podatkovne modele i komunikacijske protokole između pametnih brojila i sustava za prikupljanje podataka.
Dodatno, za komunikaciju se koriste tehnologije kao što su PLC (Power Line

Communication), GPRS/3G/4G mobilne mreže te RF mesh mreže**,** ovisno o topologiji mreže i regulatornim zahtjevima. Sigurnosni mehanizmi unutar standarda uključuju autentifikaciju uređaja, enkripciju podataka (AES) i upravljanje pristupnim pravima. Osim navedenih standarda, sigurnosni zahtjevi za sustave pametnih mreža i naprednu mjernu infrastrukturu (AMI) dodatno su definirani u smjernicama međunarodnih organizacija, poput preporuka Nacionalnog instituta za standarde i tehnologiju (NIST), koje naglašavaju upravljanje rizicima, zaštitu komunikacije i sigurnost krajnjih uređaja (NIST, 2020).

## 4. Zaključak

Zaključci u ovom radu temelje se na provedenoj komparativnoj analizi metoda očitanja te kvalitativnoj procjeni sigurnosnih rizika i mjera zaštite opisanih u prethodnim poglavljima.

U kontekstu globalne energetske tranzicije i sve veće važnosti energetske učinkovitosti, odabir optimalne metode očitanja postaje strateška odluka za energetske tvrtke. Potrebno je uzeti u obzir različite faktore, kao što su troškovi, točnost, efikasnost, angažman korisnika i sigurnost, kako bi se osigurao pouzdan i ekonomičan sustav mjerenja potrošnje energije.

Prijelomna točka isplativosti između metoda očitavanja vrlo je nisko postavljena, odnosno, metoda ljudskog izvanrednog očitanja već kod trećeg godišnjeg očitanja pokazuje kako je financijski neisplativa za korisnika. Samoočitanje je najisplativije za disciplinirane korisnike, dok je daljinsko očitanje optimalno za sve koji žele minimalnu brigu i maksimalnu automatizaciju, bez dodatnih troškova. Ljudsko očitanje opravdano je samo u iznimnim situacijama i za korisnike s vrlo rijetkim potrebama za očitavanjem.

Svaka metoda očitanja električnih brojila ima svoje specifične sigurnosne rizike. Daljinsko očitanje, iako nudi najveću praktičnost i točnost, suočava se s najkompleksnijim sigurnosnim izazovima vezanima uz kibernetičku sigurnost i privatnost podataka. Daljinsko očitanje brojila za struju donosi značajne sigurnosne prednosti, ali i nove izazove. Ključna je primjena naprednih sigurnosnih tehnologija, stalni nadzor i edukacija korisnika kako bi se rizici sveli na minimum, a sigurnost podataka i pouzdanost sustava maksimalno povećali. S aspekta sigurnosti, daljinsko očitanje predstavlja sustav s najvećim potencijalnim rizicima, ali i s najrazvijenijim mogućnostima zaštite. Primjena standardiziranih sigurnosnih protokola, višeslojnih mjera zaštite i kontinuiranog nadzora omogućuje značajno smanjenje kibernetičkih prijetnji. U usporedbi s tradicionalnim metodama, daljinsko očitanje zahtijeva veća početna ulaganja u sigurnost, no dugoročno pruža višu razinu zaštite podataka i stabilnosti sustava. Doprinos rada ogleda se u sustavnom pregledu sigurnosnih izazova i mjera zaštite u sustavima daljinskog očitanja, čime se stvara podloga za buduća istraživanja usmjerena na detaljnu tehničku i eksperimentalnu analizu ovih sustava.

## 5. Literatura

Bača, M. (2004). *Uvod u računalnu sigurnost.* Zagreb: Narodne novine.

Benzi F., Anglani N., Bassi E., Frosini L. (1. October 2011). Electricity Smart Meters Interfacing the Households. *IEEE Transactions on Industrial Electronics, 58*(10), str. 4487-4494. doi:10.1109/TIE.2011.2107713

Kim, D., Solomon, M. (2018). *Fundamentals of Information Systems Security, Third Edition.* Burlington: Jones & Bartlett Learning.

Kizza, J. M. (2017). *Guide to Computer Network Security, Fourth Edition.* UK:

Springer. doi:10.1007/978-3-319-55606-2

Luring, N., Szameitat, D., Hoffmann, S., & Bumiller, G. (2018). Analysis of security features in DLMS/COSEM: Vulnerabilities and countermeasures. *2018 IEEE Power & Energy Society Innovative Smart Grid Technologies Conference (ISGT)* (str. 1-5). Washington: IEEE. doi:10.1109/ISGT.2018.8403340

Majdandžić, N. (2004). *Izgradnja informacijskih sustava proizvodnih poduzeća.* Slavonski Brod: Strojarski fakultet.

Momoh, J. A. (2008). *Electric Power Distribution, Automation, Protection, and Control, 1st Edition.* Boca Raton: CRC Press. doi:10.1201/9781315221991

Pejić Bach, M. i. (2016). *Informacijski sustavi u poslovanju.* Zagreb, Hrvatska, Hrvatska: Ekonomski fakultet Sveučilišta u Zagrebu.

Semlambo, A. A., Mfoi, D. M., & Sangula, Y. (3. November 2022). Information Systems Security Threats and Vulnerabilities: A Case of the Institute of Accountancy Arusha (IAA). *Journal of Computer and Communications*, str. 29-43. doi:10.4236/jcc.2022.1011003

Skok, S. (2002). *Besprekidni izvori napajanja.* Zagreb: Kigen.

Stojkov, M., Baus, Z., Barukčić, M., & Provči, I. (2015). *Električni sklopni aparati.* Slavonski Brod: Strojarski fakultet u Slavonskom Brodu.

NIST (2020). *Guidelines for Smart Grid Cybersecurity (NISTIR 7628 Rev. 1).* National Institute of Standards and Technology, Gaithersburg, MD.

Gungor, V. C., Sahin, D., Kocak, T., Ergut, S., Buccella, C., Cecati, C., & Hancke, G. P. (2019). Smart grid technologies: Communication technologies and standards. *IEEE Transactions on Industrial Informatics, 15(1),* 524–534. https://doi.org/10.1109/TII.2018.2880059

Yan, Y., Qian, Y., Sharif, H., & Tipper, D. (2020). A survey on cyber security for smart grid communications. *IEEE Communications Surveys & Tutorials, 22(1),* 998–1027. https://doi.org/10.1109/COMST.2019.2947204

# ANALYSIS OF SECURITY THREATS AND PROTECTION MEASURES IN REMOTE ELECTRICITY METER READING SYSTEMS

Abstract: This paper analyses different methods of electricity consumption reading with a particular focus on security aspects and the economic feasibility of remote electricity meter reading systems. The study compares traditional manual reading, customer self-reading and remote reading based on criteria such as costs, accuracy, efficiency and data security. Special attention is given to security risks associated with remote meter reading, as well as to protection measures against cyber-attacks and their role in preserving data confidentiality and integrity. The methodology is based on a review of relevant literature and a comparative analysis of the economic feasibility of individual reading methods. The results of the analysis indicate that remote meter reading, when supported by standardised security mechanisms such as encryption and access control, provides a higher level of security and operational efficiency and represents a reliable and long-term sustainable solution, despite higher initial implementation costs.

Keywords: remote meter reading, cyber security, vulnerabilities, data protection.