Rangering av strømmålere med hensyn til helserisiko, personvern og nettsikkerhet

av Ronald M. Powell, PhD[1]

(Original: Ronald M. Powell: «Ranking Electricity Meters for Risk to Health, Privacy, and Cyber Security», pdf-notat, 3. utgave, datert 12. november 2015, oversatt av Einar Flydal, desember 2020. Enkelte steder er det tilføyd *kursiv* og [kommentarer. O.a.] for å tilpasse til norske forhold.)

Tabell 1: Sammendrag av risikorangeringene

	Målertype	**Kommunikasjonstype**				**Samlet risiko** 5 er høyest. Tom celle er lavest.		
			Trådløs	Kablet		**Helse-risiko**	**Personvern-risiko**	**Risiko mht nettsikkerhet**
G	SMARTMÅLER	WAN / HAN	✓			5	5	5
F	AMR-måler	«Putring»[2]	✓			4	4	
	Analog måler (med trådløs digital elektronikk)	«Putring»	✓			4	4	
E	AMR-måler	«Vekking»[3]	✓			3	4	
	Analog måler (med trådløs digital elektronikk)	«Vekking»	✓			3	2	
D	SMARTMÅLER	Internett kabel/fiber		✓		2	4	4
	AMR-måler	Internett kabel/fiber		✓		2	4	
C	SMARTMÅLER	Fast telefonlinje		✓		2	3	2
	AMR-måler	Fast telefonlinje		✓		2	1	
B	Enkel digital elektronisk måler	Ingen				2		
A	Tradisjonell analog måler	Ingen						
	SMARTMÅLER[4]	*PLC (strømnettet)*		✓		3	5	2

Tabell 1 oppsummerer risikorangeringen av strømmålere, basert på de detaljerte analysene som følger. «5» angir høyest risiko. Tom celle angir lavest risiko. BLOKKBOKSTAV angir en gruppe målere med lignende, men ikke nødvendigvis identisk, risikorangering.

---

1 Forfatteren, Ronald M. Powell, er en pensjonert forsker som har gjort sin karriere i USAs føderale statsadministrasjon (han har en Ph.D. i anvendt fysikk fra Harvard University, 1975). Under sin karriere i statsforvaltningen arbeidet han for presidentens Executive Office, ved the National Science Foundation, and ved the National Institute of Standards and Technology. Han kan kontaktes på (301) 926-7568, ronpowell@verizon.net.

2 [Denne kommunikasjonstypen er visstnok ikke i bruk i Norge til AMS-målere i strømnettet, men kan være i bruk i kommunale eller private målersystemer, f.eks. for vann. Man kan identifisere dem lett med et måleapparat ved å se at de pulser jevnlig. O.a.]

3 [Se fotnote 2 over. Men denne målertypen vil bare sende signaler kort etter at den er «vekket». O.a.]

4 [Denne målertypen er føyd til i den norske oversettelsen utfra oversetterens vurdering. Den brukes enkelte steder i Norge. O.a.]

Prioriteringene mellom de tre typer risiko som behandles, er slik:

- **Helse:** målerne er ordnet i synkende rekkefølge utfra helserisikoen, som er den viktigste risikofaktoren etter forfatterens mening.
- **Personvern:** målere med samme helserisiko er ordnet i synkende rekkefølge utfra personvernrisiko.
- **Nettsikkerhet:** målere med samme helserisiko og samme personvernrisiko er ordnet i synkende rekkefølge utfra risiko med hensyn til nettsikkerhet.

De trådløse smartmålerne får høyeste risikoplassering innen alle de tre risikokategoriene - i motsetning til de tradisjonelle analoge målerne, som får lavest risikoplassering innen alle de tre risikokategoriene. Analoge målere omtales også korrekt som:

- Tradisjonell analog mekanisk måler
- Tradisjonell analog elektromekanisk måler
- Tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet
- Tradisjonell analog mekanisk måler uten elektroniske kretser.

Innledning

Produsentene av strømmålere tilbyr et bredt utvalg modeller, og mange av disse modellene er tilgjengelige med et dusin eller så mulige tilvalg, noe som fører til mange mulige kombinasjoner. Disse målerne besitter evner som går utover det som er nødvendig for å måle elektrisitetsforbruket så lenge hensikten er å utstede en månedlig avregning. Dessverre innebærer de nye mulighetene en mengde risiki med hensyn til helse, personvern, og nettsikkerhet, noe som har vært mye diskutert andre steder. Disse forklares kort i følgende punkter:

- **Helserisikoen** oppstår først og fremst av det faktum at mange strømmålere kommuniserer trådløst med strømselskapene. De sender radiofrekvent stråling ved mikrobølgefrekvenser, dag og natt, hver dag hele året, for alltid. Denne strålingen går lett tvers gjennom private hjem og bedrifter, går rett gjennom både ufødte, barn og voksne, og forstyrrer helsen. Hver måler i lokalsamfunnet som er utstyrt med en sender, gjennomstråler alle i dette lokalsamfunnet. Det samme gjør hver lokalt plasserte sende- og mottakspunkt som kraftselskapene har satt opp for å kommsløunisere trådløst med disse målerne.
- **Risikoen for personvernet** oppstår av det faktum at mange av målere fanger opp og overfører svært detaljert informasjon om strømforbruk til enhver tid. Denne detaljerte informasjonen kan avsløre mye om de aktiviteter som finner sted inne i boliger og bedrifter. For eksempel er den tilstrekkelig til å avre når ingen er tilstede.
- **Risikoen med tanke på nettsikkerhet** oppstår til dels av det faktum at enkelte typer målere kan godta innkommende kommandoer som kan komme trådløst fra skadevoldende kilder. Mange av disse målerne er laget slik at de vil følge trådløse ordre om å slå av strøm-forsyningen til et hjem eller en virksomhet helt, eller ordre om å godta installasjon av ny programvare. Omprogrammeringen kan endre målerens handlinger og kan gjøre det uten at eierne av boligene eller bedriftene kan vite det.

De mange varianter målere som nå er i bruk, og de mange farer som målerne kan utgjøre, innebærer at det har blitt umulig for strømselskapets kunder å vite hvilke egenskaper måleren har og hvilken risiko disse egenskapene innebærer for kunden, hans/hennes familie, bedrift, eller nabolag. Kort sagt, strømselskapene har beveget seg -

- bort fra den aksepterte praksis som besto i å måle strømforbruket en gang i måneden i den hensikt å utstede en månedlig regning,
- til den mer tvilsomme praksis det er å overvåke dagliglivets aktiviteter inne i den enkeltes hjem og i bedrifter, slik disse gjenspeiler seg i deres detaljerte strømforbruk,
- for deretter å kringkaste disse detaljene ut i lufta ved hjelp av trådløs teknologi som forurenser hele lokalsamfunn med hundrevis av millioner «skurer»[5] av mikrobølgestråling hver eneste dag, for alltid.

Hensikten med dette dokumentet

Formålet med dette dokumentet er å gi en viss oversikt om hvilke typer målere som fins tilgjengelige, og den relative risikoen de utgjør. Fordi det er så mange typer tilgjengelige målere, kan ikke alle tas med her. De målerne som er tatt med i dette dokumentet, er de som jeg oftest har sett i bruk i delstaten der jeg bor, Maryland, USA. Mange, om ikke de fleste, av disse målerne er også i bruk i andre stater.

[I Norge er flere av disse typene i bruk, men ikke alle til strøm. Målere av typen «vekking» fins visstnok i bruk som kommunale vannmålere, og av typen «putring» som vannmålere i borettslag/sameier. Andre typer har vært i bruk til strøm, men er under utfasing, slik at kun de som er betegnet som SMARTMÅLER i Tabell 1 er i bruk i strømnettet. O.a.]

Hovedkonklusjoner

Bare én målertype, *tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet*, plassert i den nest siste raden i Tabell 2 på side 6, tilbyr alle de tre følgende positive egenskaper:

- ingen risiko for helsefare fra [radiofrekvent] RF-stråling, ettersom måleren ikke genererer noen RF-stråling
- ingen risiko for personvernet, ettersom måleren ikke kan fjernavleses
- ingen risiko med hensyn til personvernet, ettersom man ikke kan få adgang til måleren fra avstand, så den kan derfor heller ikke hackes.

Sett under ett, er det *den tradisjonelle analog mekaniske måleren uten trådløs kommunikasjons-mulighet* som utgjør den lavest risiko for helse, for personvern, og for nettsikkerhet. Tragisk nok er dette den måleren som mange nettselskaper i mange land, inkludert min delstat Maryland, har valgt å fjerne. [Slik er det også i Norge. O.a.]

5 [Betegnelsen «skurer» er her brukt for det engelske «burst». Ofte brukes det mer unøyaktige «pulser» på norsk. «skurer» er brukt fordi det bedre angir hva som normalt kommer: en brå, og intens mengde signaler over kort tid. O.a.]

Bare én type måler som undersøkt her, *den trådløse smartmåleren*, som er plassert i den øverste raden i Tabell 2 på side 6, har alle tre av følgende negative egenskaper:

- *høyest helserisiko* ettersom den har den høyeste maksimale sendestyrken på den utstrålte radiofrekvente energien (*RF-effekt*), og fordi den har enten det høyeste eller det nest høyeste antall skurer RF-stråling per dag, avhengig av hvilken driftsmodus den er innstilt på
- *høyest personvernrisiko*, ettersom data potensielt er tilgjengelige for det nest største antall mennesker, men med den største letthet hva gjelder tilgang til datastrømmen (fordi den er trådløs), og fordi den gir data med størst aktualitet, størst detaljrikdom (beste tidsoppløsning), og størst utvalg (de fleste typer data), noe som gjør datainnsamlingen svært påtrengende
- *høyest risiko med tanke på nettsikkerhet*, fordi måleren er potensielt tilgjengelig for den nest største antall mennesker, men også her med svært lett tilgang (siden nettet er trådløst), og fordi denne måleren er mest sårbar for å bli angrepet selv og fordi den er den målertypen som er mest i stand til selv å forårsake skade
    - fordi den inneholder en nedstengningsbryter som er i stand til å slå av all strøm til kunden når den utløses for å gjøre dette ved hjelp av et trådløst fjernkontrollert signal
    - fordi programvaren i måleren kan reprogrammeres til å utføre nye funksjoner, enten gunstige eller skadelige, helt usynlig for kunden.

Samlet sett er det *den trådløse smartmåleren* som utgjør den høyeste risikoen for helse, for personvern og for nettsikkerhet. Tragisk nok er dette den måleren som mange kraftselskaper i mange land, inkludert min delstat Maryland, har valgt å installere. [Slik er det også i Norge. O.a.]

De andre målerne som er omtalt i dette dokumentet, lander et sted mellom disse to nevnte målerne.

- Alle disse andre målerne innebærer helserisiko fra eksponering for RF-stråler, selv om det er store gradsforskjeller mellom dem.
- Alle, med unntak av én av de andre målerne, innebærer personvernrisiko.
- To av de andre målerne innebærer risiko med tanke på nettsikkerhet.

Organisering av resten av dette dokumentet

Rangering av strømmålere med hensyn på helserisiko

Tabell 2 på side 6 rangerer strømmålere utfra helserisiko, basert på egenskapene til den «Kilde til radiofrekvent (RF-)stråling» som hver enkelt måler inneholder. Alle uttrykkene som er brukt i tabellen, er beskrevet i teksten som følger umiddelbart etter.

Radene i tabellen angir hvilken «Målertype» som hver måler faller inn under, og hvilken «Kommunikasjonstype», enten trådløs eller kablet, som hver måler benytter seg av. Under overskriften «Kilder for radiofrekvent (RF-)stråling» og under ulike underoverskrifter angis i den sentrale delen av tabellen de egenskapene ved de ulike målernes stråling som er av betydning for helserisikoen.

En rød celle i krysset mellom en gitt rekke og kolonne betyr at målertypen som er angitt i kolonnen i venstre kant, inneholder den kilden til RF-stråling som er angitt i kolonneoverskriften over cellen, og at måleren medfører en helserisiko.

Den første av kolonnenes underoverskrifter angir «maks utstrålt RF-effekt» [dvs. intensitet eller «sendestyrke». O.a.] for hver RF-kilde. Vær oppmerksom på at intensitetene er gruppert fra venstre til høyre, altså fra laveste til høyeste nivåer maks utstrålt RF-effekt. Maks utstrålt RF-effekt er en av de viktigste faktorene som påvirker helserisikoen. Hvis andre faktorer er like, innebærer høyere maks utstrålt RF-effekt at det sendes ut mer RF-stråling, og desto høyere tilknyttet helserisiko.

Den andre av overskriftene under «kommunikasjonstype» angir antallet «RF-skurer per dag» (eller per måned) fra hver kilde radiofrekvent (RF-)stråling, så langt dette er kjent. Jo høyere antall skurer RF-stråling per dag, jo mer RF-stråling sendes ut. Jo høyere er dermed tilknyttet helserisiko.

Den siste kolonnen på høyre side av Tabell 2 har navnet «Samlet risiko». Den viser en rangering av helserisiko for hver rekke, altså for hver målertype og med angitt kommunikasjonstype. Rangeringen er angitt med poeng. Jo høyere tall, jo høyere er tilknyttet helserisiko. Alle tallene i de røde cellene under overskriften «Helserisiko» angir en *rangordning*. Det betyr at en måler med rang 5 byr på høyere helserisiko enn en måler med rang 4. Rang 5 angir høyest risiko, og en tom celle angir laveste risiko. Legg merke til at rangeringene ikke er kvantitative utover å angi rang. Det betyr at rangeringen ikke angir *hvor stor forskjellen mellom målerne er*. En bedre pekepinn om den kvantitative forskjellen kan man ved å se nøyere på forskjellene på maks utstrålt RF-effekt og på antall skurer RF-stråling per dag. Der er det angitt noen grove tall. I enkelte tilfeller har jeg ikke fått tak i gode tall som jeg kan vise til, men har angitt mine skjønnsmessige gjetninger, f.eks. i form av «meget lavt» eller «høyt». Hensikten har vært å angi i hvilket område jeg ville forvente at de faktiske tallene ville ligge – om de hadde vært kjent. Jeg har oppført disse tilfellene som «(ukjent)».

Legg merke til at ingen måler i Tabell 2 har risiko 1. Det skyldes i hovedsak at hver eneste strømmåler i tabellen, med unntak for den tradisjonelle analoge måleren, har minst to kilder til RF-stråling: digital elektronikk og SMPS[6]-type strømforsyning. Begge disse kildene skaper RF-stråling, selv om denne har en meget svak maks utstrålt RF-effekt. Legg merke til at jeg her antar at alle målere med digital elektronikk har slike strømforsyninger, selv om jeg ikke har kunne verifisere dette. Bare én måler, den tradisjonelle analoge måleren, har *ingen* kilder til RF-stråling. Den

6 [SMPS: switched mode power supply. Se mer forklaring seinere i dokumentet. O.a.]

fortjener derfor en tom celle for helserisiko, noe som angir at det er denne typen måler som er klart den sikreste av dem alle.

Tabell 2: Rangering av målere utfra helserisiko

Målertype	Kommunikasjons-type			Kilder til radiofrekvent (RF-)stråling						Samlet risiko 5 er høyest. Tom celle er lavest.
				Utilsiktet stråling		Tilsiktet stråling				
				Digital elektronikk	SMPS strøm-forsyning	Sender/mottaker uten nettverkstilknytning		Sender / mottaker for hjemme-nettverk (HAN)	Sender / mottaker for storområder (WAN)	
	Maks utstrålt RF-effekt ->; RF-skurer per dag ->; Trådløs|Kablet			meget lav (ukjent); høyt (ukjent)	meget lav (ukjent); høyt (ukjent)	lav (1 mW); lavt (8/mnd)	lav-middels (1-100 mW); høy (50.000/ dag)	middels (100 mW); høyt (ukjent)	høy (1000 mW); høyt [ca. 10.000/dag til maks 190.000]	**Helserisiko**
SMARTMÅLER Digital Avansert Målings-Infrastruktur (AMI)	WAN / HAN	✓								5
	Internett over kabel/fiber		✓							2
	Fasttelefon		✓							2
Digital Automatisk Måleravlesning AMR-måler	Putring	✓								4
	Vekking	✓								3
	Internett over kabel/fiber		✓							2
	Fasttelefon		✓							2
Enkel digital elektronisk måler	Ingen									2
Analog måler (med trådløs digital elektronikk)	Putring	✓								4
	Vekkes opp	✓								3
Tradisjonell analog måler	Ingen									
SMARTMÅLER[7]	*PLC (over strømnettet)*		✓							4

Beskrivelse av ulike typer strømmålere

En **smartmåler** er en nøkkel-komponent i det som kalles en **Avansert Målings-Infrastruktur (AMI)** eller et **Avansert Målings-System (AMS)**. Av den grunn omtales ofte smartmålere som AMS-målere.

En smartmåler er en digital, elektronisk enhet som overvåker strømflyten inn og ut av kundens bolig eller bedrift, og den sørger for to-veis kommunikasjon mellom kundens måler og strømselskapet. Informasjonen som sendes til strømselskapet beskriver mange egenskaper ved elektrisitetsflyten – på en svært presis måte og med svært detaljerte tidsangivelser («høy oppløsning»). Denne kommunikasjonen oppnås vanligvis med en trådløs sender og mottaker som inngår i et såkalt storområdenettverk («Wide Area Network», WAN). Måleren har derfor tilstrekkelig høy maks

7 [Denne målertypen er føyd til i den norske oversettelsen utfra oversetterens vurdering. Den brukes enkelte steder i Norge. O.a.]

utstrålt RF-effekt til å nå fram over store avstander. Det er dette WAN-nettverket som gir opphavet til de fleste av de helsemessige bekymringene knyttet til smartmålere. Det høyner samtidig bekymringene både for personvernet og for nettsikkerheten, både på grunn av det store området som dekkes av signalene, og på grunn av at alle signaler som sendes gjennom lufta er fritt tilgjengelige for alle.

Enhver smartmåler kan være, og er vanligvis, utstyrt med en enda en **trådløs** sender/mottaker, som er kjernen i et hjemmenettverk («Home Area Network», HAN) for å kommunisere trådløst med de enkelte såkalte smarte apparatene som måtte finnes i et hjem eller en bedrift. Dette høyner bekymringene for helse, personvern og nettsikkerhet ytterligere. HAN-nettverket er laget for å sende informasjon tilbake til strømselskapet om identiteten til det smarte apparatet og om bruken av det i det enkelte hjem eller bedrift. Jeg kjenner ikke til om HAN-nettverket også kan gjøre strømselskapet i stand til å kontrollere det smarte utstyret.

Kommunikasjon mellom smartmålere og strømselskap kan også oppnås med **kablede** teknologier, slik som faste telefonlinjer og internettforbindelser via kabel eller fiber, noe som i betydelig grad reduserer strålingen som smartmålerne produserer, men ikke fjerne den helt. Kablet kommunikasjon for smartmålere er ikke brukt i min delstat Maryland, så vidt jeg vet. Som et eksempel på en **kablet** installasjon, kan nevnes at i Chattanooga, Tennessee, brukes fiberoptisk kabel for å kommunisere med smartmålerne i byen.[8]

Målere for digital **Automatisk Måleravlesning** (AMR) er en annen type digital elektronisk enhet. En slik måler overvåker flyten av strøm inn og ut av kundens bolig, men vanligvis ikke med så høyt detaljeringsnivå som en smartmåler. AMR-måleren kan gi trådløs kommunikasjon, men vanligvis ikke direkte tilbake til strømselskapet. Det er vanligere at AMR-målerne kommuniserer trådløst med en servicebil i det bilen kjører forbi (såkalt «drive-by-reader») eller med en passerende kontrollør som går til fots («walk-by-reader»). Disse er utstyrt med det nødvendige elektroniske utstyret for å kommunisere med AMR-måleren. Ettersom avstanden som AMR-måleren må kommunisere over, er kortere enn det er for smartmålere, er maks utstrålt RF-effekt fra AMR-målere vanligvis lavere enn fra en smartmåler. To forskjellige typer trådløs kommunikasjon tilbys: «putring» («Bubble Up») og «vekking» («Wake up»). De er beskrevet på side 9. Hvis AMR-måleren er utstyrt for det, kan den i stedet kommunisere via kabelbasert Internett-tilknytning (enten kabel eller fiber) eller via fasttelefonen. Begge disse sistnevnte to løsningene gjør det mulig å få kommunikasjon hele veien tilbake til strømselskapet, slik at det ikke er nødvendig med noen løsning der en servicebil må kjøre rundt, eller en kontrollør må patruljere gatelangs.

En **enkel digital elektronisk måler** er den enkleste av alle de digitale elektroniske målerne. Den bruker hverken trådløs eller kablet kommunikasjonsteknologi. Slike målere må avleses av en kontrollør som må inn på kundens eiendom. Disse målerne har bare to kilder til RF-stråling – den digitale elektronikken og SMPS-strømforsyningen. De utgjør derfor en lavere helserisiko enn noen av de andre målerne. Disse målerne kan være i stand til å lagre en meget stor mengde data som samles inn mellom hver gang målingene avleses av kontrolløren, avhengig av de tilvalg (for eksempel ekstra elektronisk minne) som de måtte inneholde. Dette gir grunnlag for en viss

8 Your Gig is Here. Right here, in Chattanooga (http://www.chattanoogagig.com/). How Chattanooga beat Google Fiber by half a decade, The Washington Post, September 17, 2013. (http://www.washingtonpost.com/blogs/the-switch/wp/2013/09/17/how-chattanooga-beat-google-fiber-by-half-a-decade/).

bekymring for personvernet. Det samme gjelder også at data kan hentes ut svært raskt gjennom et elektronisk eller optisk grensesnitt som den patruljerende kontrolløren bruker for å koble seg til måleren. Men fordi en slik egenskap ikke nødvendigvis inngår, og fordi disse målerne leses av sjelden (vanligvis en gang i måneden), har jeg rangert disse målerne som at de ikke innebærer noen risiko knyttet til personvern. Disse målerne utgjør heller ingen risiko hva gjelder nettsikkerhet, siden de ikke er tilgjengelige utenfra og derfor heller ikke kan bli hacket.

En **analog måler (med trådløs digital elektronikk)** er en tradisjonell analog, mekanisk måler. Den tilsvarer en tradisjonell analog elektromekanisk måler som har blitt utstyrt med digitale elektroniske kretser. Den drives av en SMPS-strømforsyning for å gjøre måleren i stand til å ta i mot et trådløst oppvåkingssignal («Wake-Up») eller drive trådløs «putring» («Bubble-Up»). Disse egenskapene er drøftet videre på side 9. De gjør at måleren kan avleses utenfra på kort avstand av en servicebil som kjører forbi, eller av en patruljerende kontrollør, slik at avlesningen ikke behøver å foregå inne på kundens eiendom.

Den tradisjonelle analoge mekaniske måleren uten noen trådløs kommunikasjonsmulighet betegnes også som «tradisjonell analog *elektromekanisk* måler uten trådløs kommunikasjons-mulighet». Det er denne man vanligvis mener når man bruker de kortere beskrivelsene – så som *analog måler*, eller *analog mekanisk måler*, eller *analog elektromekanisk måler*. En slik måler inneholder ingen digitale elektroniske kretser og trenger dermed ikke noen SMPS-strømforsyning til elektriske kretser. Denne type måler inneholder ingen kilder til RF-stråling, hverken tilsiktet eller utilsiktet, og kan dermed ikke gi opphav til noen risiko for helsefare knyttet til eksponering for RF-stråling. Denne typen måler utgjør heller ingen risiko for personvernet, ettersom den ikke kan leses av utenfra, og den utgjør ingen risiko med tanke på nettsikkerhet, ettersom den ikke kan være eksternt tilgjengelig. Derfor kan denne målertypen heller ikke bli hacket. Disse egenskapene er angitt som tomme celler langs hele den nest nederste raden i Tabell 2 på side 6 og den nest nederste raden i Tabell 3 på side 12. De tomme cellene gjenspeiler det faktum at denne måleren er den sikreste som er tilgjengelig med tanke på helserisiko, personvernrisiko og nettsikkerhet.

Kilder til radiofrekvent (RF-)stråling

Alle kilder til radiofrekvent (RF-)stråling i strømmålere kan avgi stråling direkte til luft. Disse kildene kan også avgi elektriske strømmer med radiofrekvens rett inn i huset ledninger, eller de kan *indusere* RF elektrisk strøm i huset ledninger. [Slike induserte forstyrrelser som kan avleses som «skygger» på strømnettets sinuskurver, hører inn under betegnelsen «skitten strøm». O.a.] Denne radiofrekvente strømmen kan deretter stråle ut i lufta som radiofrekvent stråling. Kilder til stråling er beskrevet nedenfor, ordnet i stigende rekkefølge hva gjelder *maksimalt utstrålt RF-effekt* [også omtalt som *intensitet* eller mer upresist som «styrke», o.a.] De ulike kildene har svært ulike intensiteter, men likevel kan selv de minst sterke av dem – de som er oppført under kilder som gir «utilsiktet stråling«, forstyrre svært følsomme individer. Derfor kan man ikke se bort fra dem.

Kilder til **utilsiktet stråling** er kilder til radiofrekvent (RF-)stråling som stråler på grunn av sin iboende natur, ikke fordi strålingen er nødvendig for å utføre deres kommunikasjonsfunksjon:

- **Digital elektronikk** opererer ved å slå den elektriske strømmen på og av brått og i rask rekkefølge. Disse overgangene i strømmen produserer utilsiktet radiofrekvent stråling, dette

skjer uavhengig av om den samme elektronikken også produserer tilsiktet radiofrekvent stråling for trådløs kommunikasjon, eller ikke. Den utilsiktede strålingen fra den digitale elektronikken har vanligvis svakere maks RF-effekt og høyere frekvens enn den utilsiktede RF-strålingen fra SMPS-strømforsyningen.

- **SMPS-strømforsyninger** omformer den høye innkommende spenningen fra det elektriske strømnettet til den lavere spenningen som er nødvendig til å fóre digitale elektroniske kretser. Under denne konverteringen slår denne typen strømforsyninger den elektrisk strøm på og av brått og i rask rekkefølge. Disse overgangene i strømmen produserer utilsiktet radiofrekvent stråling. Denne utilsiktede strålingen har vanligvis sterkere maks RF-effekt, og har lavere frekvens, enn den utilsiktede RF-strålingen fra digital elektronikk. (SMPS står for «Switched Mode Power Supply» eller «Switching-Mode Power Supplies».) [En SMPS-strømforsyning er altså en *transformator*. All digital elektronikk som bruker strøm fra strømnettet – så som TV-apparater, ladere, LED-pærer, dimmere, PCer, osv. – bruker SMPS-strømforsyninger. På svensk brukes betegnelsen *pulserande strömförsörjning*. O.a.]

Kilder til **tilsiktet stråling** er kilder til radiofrekvent stråling som må stråle for å utføre sin tilsiktede funksjon – i dette tilfellet å overfør informasjon i et trådløst kommunikasjonssystem.

Kategorien **Sender/mottaker uten nettverkstilknytning** omfatter både «putring» («Bubble-Up») og «Vekking» («Wake-Up») som kommunikasjonstyper for strømmålere. Disse to typene kommunikasjon blir noen ganger betegnet under ett som ERT-kommunikasjon, der ERT står for «encoder, receiver, transmitter», altså «innkoder, mottaker, sender». Slike målere er ikke koblet sammen i nettverk.

- Målere som bruker «**putring**», sender sine måleravlesninger som trådløse signaler hver sekund eller så, hele dagen og hele natten lang, hver dag hele året. Hensikten med slike hyppige sendinger er å sikre at et signal er tilgjengelig i det øyeblikket en servicebil kjører forbi – eller en kontrollør fra strømselskapet går forbi – med elektronisk avlesningsutstyr som kan plukke opp og lagre den informasjonen som overføres av signalet. Putringsbaserte målere tilbys med *lav eller middels maksimal utstrålt RF-effekt*. Jeg har ennå ikke funnet ut om det fins putringsbaserte målere som har en mottaker for andre formål, for eksempel for å ta imot endringer i målerens interne programvare.
- Målere basert på «**vekking**» inneholder mottakere som lytter etter et trådløst signal («Wake-Up signal») som blir sendt ut fra en servicebil som kjører forbi, eller fra en kontrollør som går forbi. Deretter svarer måleren med en rekke sendinger som inneholder målerinformasjon. Åtte slike overføringer, umiddelbart etter hverandre, synes å være vanlig. Vekkingsbaserte målere overfører ikke noe som helst i tidsrommet mellom slik vekkinger. Så vidt jeg har funnet, fins vekkingsbaserte målere kun med *lav maksimal utstrålt RF-effekt*. På grunn av deres sjeldne overføringer og deres lave maks utstrålt RF-effekt, produserer vekkingsbaserte målere mye mindre radiofrekvent stråling enn putringsbaserte målere.

Sender/mottaker-enheten for hjemmenettverk (Home Area Network, HAN) er et av to trådløse to-veis kommunikasjonssystemer som vanligvis, men ikke alltid, er innebygget i trådløse smartmålere. HAN-nettverket kalles noen ganger for Zigbee-nettverk, etter teknologien som dette

nettet gjerne er basert på. HAN-systemet er utformet for å kommunisere med nye såkalte smarte apparater i ethvert hjem eller bedrift. Formålet er å overvåke disse apparatene for å overføre informasjon om deres identitet og aktiviteter tilbake til strømselskapet [og bruke slik informasjon til å tilby tjenester for styring, overvåking etc. av disse, o.a.]. Det er mulig, men jeg vet ennå ikke sikkert, at HAN-nettverket vil gjøre det mulig for strømselskapene å utøve en viss grad av ekstern kontroll over smart utstyr. HAN-nettverket sender ved hjelp av RF-stråling (med mikrobølge-frekvenser) med en middels høy maksimalt utstrålt RF-effekt. Jeg har ennå ikke funnet data på hvor ofte HAN-systemet sender sine skurer med RF-stråling, men jeg mistenker hyppigheten for å være høy, i likhet med andre typer lokale nettverk (LAN/WiFi). Alt etter svaret på dette, kan strålingen som skapes av HAN-nettverket konkurrere med, eller overstige, strålingen som produseres av WAN. [Det ser ut til at HAN-nettverk ikke er bygget inn i de smartmålerne som utplasseres i Norge, men at det må settes inn en egen tilleggsmodul, men dette er usikker informasjon. O.a.]

Et **storområdenettverk** (WAN, Wide Area Network) er en trådløs metode for to-veis kommunikasjon mellom smartemålere. Det har vanligvis form av et såkalt *maskenettverk* [engelsk: mesh network. O.a.]. WAN overfører RF-stråling (ved mikrobølgefrekvenser) med en høy maks utstrålt RF-effekt. Strålingen har dermed lang rekkevidde, derav betegnelsen «wide» i «Wide Area Network». I et slikt nettverk kommuniserer smartmålerne med hverandre hele tida. Hver enkelt smartmåler sender informasjon om bruken av elektrisitet i hjemmet eller bedriften som den først og fremst betjener. Men hver enkelt smartmåler formidler dessuten informasjon fra smartmålerne i nærliggende boliger og bedrifter. Denne videreformidlingen bidrar til å sikre at informasjonen etter hvert kommer fram til de lokale mottaker-/senderne som strømnettselskapet har i området, og som deretter sender informasjonen tilbake til selskapet ved hjelp av en eller annen av en rekke mulige metoder. Den intense graden av kommunikasjon som brukes i disse maskenettverkene fører til fra 10 000 skurer med RF-stråling per dag fra hver måler (i gjennomsnitt) opp til 190 000 skurer med RF-stråling per dag (maksimalt) fra hver måler.[9] [De smartmålerne som brukes i Norge, er oftest konfigurert for maskenett. Antallet skurer per døgn er kalkulert utfra målinger av EMF-Consult til for Kamstrup: 164 skurer per døgn, for Nuri: 4 320 skurer per døgn, og for Aidon til 83 130 skurer per døgn. Når målerne er satt opp for mobildata (GPRS), sender de – litt avhengig av dekningsforhold – i underkant av 200 skurer per døgn. O.a.] Gjennom slike intense kommunikasjonsnivåer kan skurer med RF-stråling teppelegge hele det nabolaget som er utstyrt med smartmålere, og nå opp fra millioner til hundrevis av millioner skurer med RF-stråling per dag. Da teller vi ikke med de skurene som sendes ut over hele lokalsamfunnet fra de lokale sender- og mottakerne som er satt opp av strømselskapet for å kommunisere med smartmålerne i området. Jeg har ennå ikke funnet noen data for maksimalt utstrålt RF-effekt fra slike sendere/mottakere, eller hvor mange skurer med RF-stråling de sender per dag.

9 Pacific Gas and Electric Company's Response to Administrative Law Judge's October 18, 2011 Ruling Directing it to File Clarifying Radio Frequency Information, page 5. (http://emfsafetynetwork.org/wp-content/uploads/2011/11/PGERFDataOpt-outalternatives_11-1-11-3pm.pdf)

Nivåer på maksimalt utstrålt RF-effekt

I dette dokumentet er maksimalt utstrålt RF-effekt delt inn i fire nivåer:

- «Svært lav» effekt betyr maks utstrålt RF-effekt godt under 1 milliwatt (mW)
- «Lav» effekt betyr maks utstrålt RF-effekt på 1 milliwatt (mW)
- «Middels» effekt betyr maks utstrålt RF-effekt på 100 milliwatt (mW)
- «Høy» effekt betyr maks utstrålt RF-effekt på 1 000 milliwatt (mW), som er det samme som 1 Watt (W) maks utstrålt RF-effekt

[I Norge er maks grense for utstrålt RF-effekt satt i fribruksforskriften til 0,5 Watt, målt med målemetoden e.r.p. Dette tilsvarer nesten rammen på 1 Watt i teksten over, dersom man i USA har brukt utregningsmetoden e.i.r.p., noe jeg ikke har klart å finne ut. Forskjellen har uansett ikke invirkning på rangeringene i dette dokumentet. O.a.]

Kablede kommunikasjonsmåter

Noen smartmålere, og noen AMR-målere, kan være utstyrt for å sende informasjon tilbake til strømselskapet gjennom *kablede kommunikasjonssystemer*. Disse systemene bruker ikke tilsiktet stråling og gir dermed ikke grunn for bekymringer for helserisiko knyttet til tilsiktet RF-stråling. Imidlertid benytter disse målerne fortsatt digital elektronikk og SMPS-strømforsyning, slik at også disse kommunikasjonssystemene øker nivået utilsiktet RF-stråling i miljøet. To typer kablede kommunikasjonssystemer er omtalt i dette dokumentet:

- «Internett» [«bredbånd»] kan brukes via kabelbaserte teknologier, slik som koaksialkabel og fiberoptisk kabel [eller som ADSL via fasttelefonisystemets kobberledninger. O.a.].
- «Telefonledningene» kan brukes, hva enten de er basert på kobberledninger, koaksialkabel eller fiberoptisk kabel.

[I Frankrike brukes *kommunikasjon over strømledningsnettet* – PLC (Power Line Communication – som standardløsning for nye strømmålere. I Norge brukes PLC som teknisk løsning av noen få strømselskaper. Smartmåler med PLC er derfor lagt til som en siste rad i tabellene. O.a.]

Rangering av strømmålere utfra personvernrisiko og med hensyn til nettsikkerhet

Tabell 3 på side 12 tar for seg de samme målertypene og de samme kommunikasjonstypene som er angitt i Tabell 2 i forbindelse med helserisiko. Men i Tabell 3 handler det om personvernrisiko, og om risiko knyttet til nettsikkerhet. For å lette sammenligningen er de samlede resultatene for helserisiko fra Tabell 2 gjengitt i kolonnen på høyre side av Tabell 3. Der vises samlet risiko for alle tre: helse, personvern og nettsikkerhet.

Tabell 3: Rangering av strømmålere utfra risiko for personvern og nettsikkerhet
(RØD betyr helserisiko, BLÅ personvernrisiko, GRØNN betyr risiko mht nettsikkerhet)

Målertype	Kommunikasjons-type			Risiko for personvernet					Risiko mht nettsikkerhet			Samlet risiko 5: høyest. Tom celle: lavest.		
				Fjerntilgang til datastrøm		Dataenes art			Fjerntilgang til måler					
	Rangeringskriterier →	Trådløs	Kablet	Antall folk med mulig fjerntilgang	Hvor lett det er å få fjernadgang	Hvor ferske data?	Detaljeringsnivå	Variasjonsbredde	Antall folk med mulig fjerntilgang	Hvor lett det er å få fjernadgang	Målerens sårbarhet med hensyn til å bli skadet eller å gjøre skade	Helserisiko	Risiko for personvern	Risiko med hensyn til nett sikkerhet
SMARTMÅLER Digital Avansert Målings-Infrastruktur (AMI)	WAN / HAN	✓		4	5	5	5	5	4	5	5	5	5	5
	Internett over kabel/fiber		✓	5	2	5	5	5	5	2	5	2	4	4
	Fasttelefon		✓	1	1	1	5	5	1	1	5	2	3	3
AMR-måler Digital Automatisk Måler-Avlesning	«Putring»	✓		3	5	5	5	2	3	5		4	4	
	«Vekking»	✓		2	5	1	1	2	2	5		3	2	
	Internett over kabel/fiber		✓	5	2	5	5	2	5	2		2	4	
	Fasttelefon		✓	1	1	1	1	2	1	1		2	1	
Enkel digital elektronisk måler	Ingen					1	1	1				2		
Analog måler (med trådløs digital elektronikk)	«Putring»	✓		3	5	5	5	2	3	5		4	4	
	«Vekking»	✓		2	5	1	1	2	2	5		3	2	
TRADISJONELL ANALOG MÅLER	Ingen													
SMARTMÅLER[10] (AMI)	*PLC (over strømnettet)*		✓	4	2	5	5	5	5	2		4	5	4

10 [Smartmåler med PLC-kommunikasjon er føyd til i den norske oversettelsen og gitt rangering utfra Powells kriterier og vurderinger. Denne typen kommunikasjon brukes enkelte steder i Norge. O.a.]

Kriterier for alle rangeringer

Det er mange egenskaper ved hver strømmåler som påvirker risikoen som strømmåleren utgjør for helse, personvern, og nettsikkerhet. Dessverre er informasjon om mange av disse kjennetegnene ikke offentlig tilgjengelig. De egenskapene som det i det minste er *noe* tilgjengelig informasjon om, og som jeg har valgt å bruke her, er vist i kolonneoverskriftene i Tabell 3.

Det er fullt forståelig at det kan være berettiget uenighet om hvordan man skal rangere risikoen, om ikke annet så fordi det fins mange mulige forskjellige konfigurasjoner, selv for en enkel strømmåler-modell, og fordi det må utøves et visst skjønn for å lage en risikorangering. Men likefullt er det mitt håp at den samlede rangeringen som presenteres her vil være nyttig for i det minste å identifisere:

- Den målertypen som gir høyest risiko
- Den målertypen som gir lavest risiko
- De målertypene som ligger i mellom, selv om det er uenighet om rangeringen innen disse

Her er kriteriene som jeg har brukt for å rangere risikoen innen hver av de tre risikokategoriene:

Helserisiko

Helserisikoen er høyere når RF-strålingen som skapes, er høyere. Og RF-strålingen er høyere når **maksimalt utstrålt RF-effekt** er høyere, og når **antall skurer med RF-stråling** per dag er høyere, så lenge andre faktorer er like.

[De AMS-målerne som brukes i Norge, har adaptive antenner, dvs. at de alt etter forholdene sender med skiftende *utstrålt effekt*, også kalt *utgangseffekt*, *intensitet*, eller «styrke». Utstrålt effekt kan variere f.eks. dersom det kommer hindringer i veien mellom målere, og de går til maks effekt i en periode rett etter strømbrudd, når maskenettet skal re-konfigurere seg. Det er standard målemetode å foreta risikovurderinger av eksponeringen utfra *maksimal* effekt, og ikke utfra gjetninger eller målinger av hvor lav utstrålt effekt kan tenkes å bli. O.a.]

Maksimalt utstrålt RF-effekt

Risiko	Høy maksimalt utstrålt RF-effekt (1 Watt)
↑	Middels maksimalt utstrålt RF-effekt (100 milliwatt)
	Lav maksimalt utstrålt RF-effekt (1 milliwatt)
	Ingen RF-stråling

Når maksimalt utstrålt RF-effekt var ukjent, slik den var for digital elektronikk og SMPS-strømforsyninger, i Tabell 2 på side 6, gjorde jeg et begrunnet, men kvalitativ gjetning, og satte den i disse tilfellene til «meget lav» og anførte at den var «ukjent».

Antall skurer med RF-stråling

Risiko	Høyt antall skurer med RF-stråling per dag (mer enn 10 000 per dag)
↑	Middels antall skurer med RF-stråling per dag (Det var ingen målere i denne gruppen, så jeg definerte ikke noe kriterium)
	Lavt antall skurer med RF-stråling per dag (8 per måned)
	Ingen skurer med RF-stråling

Når antall skurer med RF-stråling per dag var ukjent, slik den var for hjemmenettverk (HAN) i Tabell 2 på side 6, gjorde jeg et begrunnet, men kvalitativ gjetning, og satte den i disse tilfellene til «høy» og anførte at den var «ukjent».

[Vi ser at de «norske» smartmålerne vil fordele seg slik: Aidon vil havne i gruppen «Høyt», mens Kamstrup og Nuri vil havne i gruppen «middels». O.a.]

Antall mennesker som eksponeres av strålingen

Helserisikoen øker også for samfunnet forøvrig når flere mennesker eksponeres for stråling. Antall personer som er eksponert for stråling, er større når maksimalt utstrålt RF-effekt er høyere, ettersom størrelsen på området som utsettes for stråling da øker og dermed omfatter flere personer. Så

maksimalt utstrålt RF-effekt spiller minst to roller i risikobildet: Den både øker risikoen for hver enkelt person og øker antallet personer som får høyere risiko. Derfor er det ikke noen egen overskrift «Antall personer utsatt for stråling» i Tabell 2 på side 6.

Risiko	Høyest antall personer nås ved maksimalt utstrålt RF-effekt (1 Watt)*
↑	Middels antall personer nås ved maksimalt utstrålt RF-effekt (100 milliwatt)
	Lavt antall personer nås ved maksimalt utstrålt RF-effekt (1 milliwatt)
	Ingen personer nås ved maksimalt utstrålt RF-effekt lik null.

[* Se kommentar om målemetode for Watt-styrken på s. 11.]

Personvernrisiko

De kriteriene som påvirker risikoen for personvernet, er ulike for de ulike «publikum» som dataene har. Med publikum mener jeg folk som mottar og undersøker dataene, og går inn i noen andres private sfære. Her tenker jeg på to ulike «publikum»:

- personer *utenfor* strømselskapet
- strømselskapet selv.

For folk utenfor strømselskapet, kan personvernrisikoen oppfattes som avhengig av to kriterier:

- ekstern tilgang til datastrømmen
- dataenes art.

For strømselskapet, som har full tilgang til alle data som oversendes fra selskapets strømmålere, er ikke tilgang til dataene et problem. Derfor er det kun dataenes art som er relevante i dette tilfellet. Jeg har derfor overveid hva strømselskapet kan gjøre med dataene som samles inn, som for eksempel å utlevere dem til andre utenfor strømselskapet, noe som er en erkjent offentlig bekymring. Dette er en ukjent faktor som jeg ikke fant å kunne tallfeste her. Hvis dette skulle skje, ville det helt klart være en overordentlig alvorlig sak.

Tabell 3 på side 12 kan brukes til å anslå risikoen for personvern fra begge kategorier publikum, ettersom kriteriene har vært delt i to hovedkategorier slik jeg nettopp har beskrevet. Imidlertid er den generelle «Risiko for personvern», som er angitt på høyre side av tabellen, et uttrykk for begge kategoriene, og tar derfor utgangspunkt i at publikum er folk *utenfor* strømselskapet. Ser vi på risikorangeringen under «Dataenes art» alene, kan den generelle risiko for personvernet i like høy grad knyttes til strømselskapet, som til folk utenfor strømselskapet, eller i enda høyere grad.

Fjerntilgang til datastrømmen

Risikoen for personvernet øker med antall mennesker som potensielt kan få tilgang til data-strømmen, og med hvor enkelt det er å få slik tilgang. Med tilgang til datastrømmen mener jeg tilgang til den gjennom systemet som måleren inngår i – ikke tilgang man får ved fysisk å kutte i en ledning, kabel, eller en fiber.

Risiko ↑	En datastrøm over trådbundet internett (hva enten kabel eller fiber) gir størst antall personer mulig ekstern tilgang til datastrømmen.
	En trådløs datastrøm gir et middels antall personer mulig ekstern tilgang til datastrømmen.
	Kablet fasttelefonlinje gir det minste antall personer mulig ekstern tilgang til datastrømmen.
	Ingen datastrøm gir ingen tilgang

I de tilfellene der «ingen datastrøm» gjelder, er det ingen risiko for personvernet, uansett hvordan de andre kriteriene som er knyttet til personvern, er rangert. Dette gjelder for tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet, og for enkel digital elektronisk måler.

Hvor lett det er å få fjernadgang til datastrømmen

Risikoen for personvernet øker også med hvor lett det er for folk med fjernadgang til måleren også å få adgang til datastrømmen.

Risiko ↑	Trådløse datastrømmer er lettest å få ekstern tilgang til, ettersom de går gjennom luften.
	Trådbundet internett (hva enten kabel eller fiber) er det mindre lett å få ekstern tilgang til.
	Kablet fasttelefonlinje er den forbindelsen som er minst lett å få ekstern tilgang til.
	Ingen ekstern datastrøm gir ingen fjernadgang

I de tilfellene der det ikke fins noen ekstern datastrøm, er det ingen risiko for personvernet, uansett hvordan de andre kriteriene som er knyttet til personvern er rangert. Dette gjelder bare for tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet, og for enkel digital elektronisk måler. Disse har hverken trådløs eller trådbundet kommunikasjonsmulighet.

Dataenes art

Dataenes kjennetegn påvirker i hvilken grad de vil være nyttige for den som vil krenke personvernet.

Hvor ferske er dataene?

Data som er ferske, har høyere sannsynlighet for å være nyttige for den som vil krenke personvernet.

Risiko ↑	Ferske data er mer nyttige for personvernkrenkelser.
	Gamle data er mindre nyttige for personvernkrenkelser.

Detaljeringsgrad

Data som har høyere tidsoppløsning (større detaljeringsgrad), har høyere sannsynlighet for å være nyttige for den som vil krenke personvernet.

Risiko ↑	Data med høyere oppløsning (målinger på flere tidspunkter) er nyttigere for personvernkrenkelser.
	Data med lavere oppløsning (målinger på flere tidspunkter) er mindre nyttig for personvernkrenkelser.

Variasjonsbredde

Høyt antall ulike slags data har høyere sannsynlighet for å være nyttige for den som vil krenke personvernet.

Risiko ↑	Flere datatyper er nyttigere for personvernkrenkelser.
	Færre datatyper er mindre nyttig for personvernkrenkelser.

Risiko med hensyn til nettsikkerhet

Merk at jeg bruker uttrykket «nettsikkerhet» i svært begrenset betydning i dette dokumentet. Uttrykket refererer til målerens sikring mot signaler utenfra

- som kan forstyrre måleren selv (for eksempel ved å endre dens målinger eller ved å endre dens interne programmering)
- som kan føre til at måleren gjør skade utenfor seg selv (for eksempel, ved å stenge ned all strømforsyning til kunden).

Jeg har ikke vurdert nettsikkerhet i den forstand at måleren kan tjene som en inngangsport til nettverket som måleren er en del av, og så gjøre skade gjennom dette nettverket. Hvorvidt det er mulig, kjenner jeg ikke til. Hvis det er mulig, ville det være en overordentlig alvorlig sak.

Jeg har heller ikke vurdert nettsikkerheten med tanke på at nettselskapets lokale sendere/mottakere kan tjene som inngangsporter til nettverket. Også dette ligger utenfor det jeg har kjennskap til. Hvis dette er mulig, vil også dette være en overordentlig alvorlig sak.

Antall personer med mulig fjerntilgang til måleren

Risikoen med hensyn til nettsikkerhet øker med antall personer som har mulig fjerntilgang til måleren.

Risiko ↑	Trådbundet internett (hva enten kabel eller fiber) gir størst antall personer mulig ekstern tilgang til måleren.
	En trådløs datastrøm gir et middels antall personer mulig ekstern tilgang til måleren.
	Kablet fasttelefonlinje gir det minste antall personer mulig ekstern tilgang til måleren.
	Ingen fjerntilgang gir ingen ekstern tilgang.

I de tilfellene der det ikke fins noen fjerntilgang, er det ingen risiko med hensyn til nettsikkerheten, uansett hvordan de andre kriteriene som er knyttet til nettsikkerhet er rangert. Dette gjelder bare for tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet, og for enkel digital elektronisk måler.

Hvor lett det er å få fjerntilgang til måleren

Risiko med hensyn til nettsikkerheten øker med hvor lett det er å få fjerntilgang til måleren.

Risiko ↑	Målere med trådløs kommunikasjon er det enklest å få ekstern tilgang til, ettersom signalene går gjennom lufta.
	Målere med kablet internettforbindelse (hva enten kabel eller fiber) er det mindre enkelt å få ekstern tilgang til.
	Målere med kablet fasttelefonlinje er det mindre enkelt å få ekstern tilgang til.
	Målere uten noen ekstern tilgang.

I de tilfellene der det ikke fins noen fjerntilgang, er det ingen risiko med hensyn til nettsikkerheten, uansett hvordan de andre kriteriene som er knyttet til nettsikkerhet er rangert. Dette gjelder bare for tradisjonell analog mekanisk måler uten trådløs kommunikasjonsmulighet, og for enkel digital elektronisk måler. Ingen av dem har noen trådløs eller trådbundet kommunikasjonsmulighet.

Målerens sårbarhet med hensyn til å bli skadet eller skade

Risiko med hensyn til nettsikkerheten øker med hvor lett det er for måleren å bli skadet eller å gjøre skade.

Risiko ↑	Måleren har en intern nedstegningsbryter. (Alltid når slike fins, kan de fjernstyres.)
	Måleren har en intern nedstegningsbryter.
	Måleren kan nås utenfra, men har ingen mulighet for å handle på ordre fra signaler utenfra.

Risiko ↑	Måleren har intern programvare som kan omprogrammeres fra avstand.
	Måleren har ingen intern programvare, eller har intern programvare som ikke kan omprogrammeres fra avstand.
	Måleren kan nås utenfra, men har ingen mulighet for å handle på ordre fra signaler utenfra.

Hvis måleren ikke kan handle på ordre fra signaler utenfra, er den ikke sårbar i den betydning som er ment her. En rekke av de målerne som er omtalt i dette dokumentet, ser ut til å være usårbare i denne betydningen, slik det går fram i Tabell 3 på side 12.

Begrensninger ved denne analysen

Denne analysen har mange begrensninger:

- Det fins så mange varianter strømmålere tilgjengelig at ikke alle er omtalt her.
  - Antall varianter øker ytterligere ved at det for en del av målerne fins mange valgmuligheter på maskinvaresiden og ved at de kan programmeres.
  - Noen av maskinvareendringene kan utføres av nettselskapene før eller etter installasjon, ikke bare av produsentene.
  - Noen av programmeringsmulighetene kan utnyttes ikke bare før installasjon, men også etter installasjon, og til og med fra avstand etter installasjon [fjernoppdatering, o.a.]. Dermed kan programvarens egenskaper endres usynlig for kunden.
- Risikoen som er angitt her, er svært avhengig av de [utstyrs- og programmerings-]valg som inngår i den enkelte måler. Generaliseringene som er gjort her om en bestemt type måler, kan derfor gjelde i større eller mindre grad, avhengig av disse valgene.
- Det utvikles nye målere hele tida.
- Det er umulig å få tak i all den informasjonen som er relevant for å kunne vurdere risikoen ved målerne med hensyn på helse, personvern og nettsikkerhet. Dette gjelder for alle målere, og av flere grunner:
  - Noe av informasjonen som er nødvendig, oppfattes som konfidensiell og proprietær [altså konkurranseføIsom informasjon, o.a.]
    - av målerprodusentene
    - av testlaboratoriene som skal påvise at målerne overholder reguleringsbestemmelsene til Federal Communications Commission i USA [i Norge: til EUs CE-sertifisering i Norge, o.a.].
    - av nettselskapene som kjøper og installerer målerne hos sine kunder.
  - Noen produsenter og strømselskaper avslår å legge fram informasjon om målerne, selv om denne informasjonen ikke formelt sett er ansett som konfidensiell eller proprietær. Vanligvis får man ingen begrunnelse.
  - Noe av den nødvendige informasjonen er aldri kartlagt.
  - Selv for informasjon som fins, kan det være slik at det ikke fins noe rettslig krav om at denne informasjonen skal legges fram for offentligheten uten en rettslig kjennelse. En slik kjennelse er blir brukt i minst ett tilfelle, og framskaffet vesentlig informasjon om smartmålere som det tidligere ikke hadde vært mulig å få fram.[11]

[I Norge kan man bruke Miljøklagenemnda eller rettslige krav for å få fram relevant informasjon. O.a.]

Avslutning

Trass i denne analysens begrensninger håper jeg at dette dokumentet kommer tett nok på virkeligheten til at det fanger opp de viktigste forskjellene blant de mange typer målere som blir omtalt her, slik at dokumentet kan gi et nyttig perspektiv på målernes relative risiko. Og kanskje dette dokumentet vil motivere dem som vet mer om målere enn jeg gjør, til å utvikle sin egen rangering.

---

11 Pacific Gas and Electric Company's Response to Administrative Law Judge's October 18, 2011 Ruling Directing it to File Clarifying Radio Frequency Information, page 5. (http://emfsafetynetwork.org/wp-content/uploads/2011/11/PGERFDataOpt-outalternatives_11-1-11-3pm.pdf)