dialogic
innovatie • interactie

Mogelijkheden voor het aanpassen van de frequentie-instelling van slimme meters in de PAMR-band

Slimme meters van Alliander, Stedin en Westland Infra maken gebruik van het CDMA-netwerk van Utility Connect, dat werkt in de PAMR-frequentieband. EZK heeft zich voorgenomen deze band te verkavelen. Dit vereist een aanpassing van de frequenties die het netwerk en de slimme meters voor de CDMA-communicatie gebruiken. In dit onderzoek wordt uitgezocht of deze wijziging op afstand door te voeren is in de betreffende slimme meters en wat hiervan de risico's zijn.

Ir. Tommy van der Vorst & ir. Jan van Rees

Opdrachtgever:
Ministerie van Economische Zaken en Klimaat

Publicatienummer:
2021.126-2135 v1.0.40

Datum:
Utrecht, 7 maart 2022

Inhoudsopgave

Citeren als: Dialogic, van der Vorst, Tommy, van Rees, Jan (2022). *Mogelijkheden voor het aanpassen van de frequentie-instelling van slimme meters in de PAMR-band.* Ministerie van Economische Zaken, Den Haag.

1 Inleiding

Het Ministerie van Economische Zaken en Klimaat (EZK) heeft Dialogic gevraagd onderzoek uit te voeren naar de mogelijkheden voor het wijzigen van de kanaalinstelling van slimme meters in de PAMR-band.

Achtergrond

Een aantal jaar geleden zijn de Nederlandse netbeheerders gestart met de uitrol van slimme meters. Deze meters worden via een draadloos netwerk uitgelezen. Alliander, Stedin en Westland Infra maken gebruik van een CDMA-netwerk, geëxploiteerd door Utility Connect. Dit netwerk maakt gebruik van (vergunde) frequentieruimte bestemd voor PAMR (*public access mobile radio*) tussen de 450 -470 MHz.[1] Andere netbeheerders gebruiken andere (openbare) netwerken.

De vergunning aan Utility Connect voor het gebruik van dit spectrum werd in 2005 verleend en gold tot en met 17 november 2020. [1] In november 2018 werd besloten dat de vergunning met vier jaar kon worden verlengd tot en met 17 november 2024. [2] In maart-april 2021 heeft EZK een beleidsvoornemen geconsulteerd over het toekomstig gebruik van de PAMR-frequentieband. Onderdeel van dit voornemen is het splitsen van de huidige PAMR-band in twee kavels/vergunningen van ieder 1,5 MHz gepaard spectrum. Het 'lager' gelegen kavel 'A' zal beschikbaar blijven voor de huidige vergunninghouder, en het hoger gelegen kavel 'B' zal zoveel mogelijk technologie- en dienstenneutraal uitgegeven worden.

Dialogic onderzocht eerder hoe de verschillende mogelijkheden ten aanzien van de PAMR-band zich verhouden tot continuïteit van de slimme meter. [3] In dit onderzoek wordt onder andere geconcludeerd dat het overstappen naar een andere (modernere) netwerktechnologie kostbaar is. Er is ten minste één CDMA-carrier (en in dat geval ook investeringen in het netwerk) nodig om de slimme CDMA-meters te kunnen blijven uitlezen. Het eerdere onderzoek presenteert diverse mogelijkheden voor het anders inrichten van de PAMR-band, waarbij wordt aangegeven dat een voor de hand liggende mogelijkheid is om naast een CDMA-kavel ook een kavel te definieren dat kan worden ingezet voor (bijvoorbeeld) LTE-M.

De CDMA-kanalen die de betreffende meters op dit moment gebruiken, 107 en 157, liggen binnen respectievelijk kavel A en B (waarbij kanaal 107 aan de rand van kavel A ligt). Om te voorkomen dat de gebruiksmogelijkheden voor kavel B worden ingeperkt, zou het gebruikte kanaal moeten worden aangepast. Hiervoor is een zogenoemde 'PRL-update' noodzakelijk op de (modemmodule van) de betreffende slimme meters.[2]

In haar reactie op de consultatie [4] hebben Alliander, Stedin en Westland Infra aangegeven dat de CDMA-meters van CDMA-kanaal 107 en/of 157 gebruik moeten blijven maken om de continuïteit van de slimme meter te borgen. Zij geven aan dat een PRL-update voor een deel van de meterpopulatie in de praktijk niet mogelijk is, en dat er daarnaast onzekerheden zijn.

Onderzoeksvragen

De vraag die in dit onderzoek centraal staat, is de volgende:

> *In hoeverre kunnen netbeheerders de kanaalinstelling in de slimme meters op afstand aanpassen?*

Wij voegen hieraan toe dat belangrijk is om voorafgaand aan het beantwoorden van deze vraag met zekerheid vast te stellen *of* een aanpassing op afstand wel noodzakelijk is. Dit is afhankelijk van de huidige instelling (PRL, zie verderop). Het is denkbaar dat deze andere kanalen toestaat dan de nu gebruikte (en dat de gehanteerde PRL per model of revisie van de slimme meter verschilt).

De netbeheerders connecteren ook andere apparatuur via het CDMA-netwerk, zoals ten behoeve van het schakelen van straatverlichting en het uitlezen van midden- en laagspanningsinstallaties. Deze vallen buiten de scope van deze opdracht, maar ook van

[1] De vergunning aan Utility Connect betreft het spectrum tussen 451,76–454,77 MHz en 461,76–464,76 MHz.

[2] Wanneer kavel B niet meer kan worden gebruikt voor het connecteren van de slimme meters, zendt het CDMA-netwerk niet meer uit in kanaal 157. Er is geen update op de slimme meter nodig om te voorkomen dat deze van dit kanaal gebruik blijven maken. Een update kan wel nodig zijn om te voorkomen dat de meters lang blijven 'zoeken' naar een netwerk in dit kanaal.

deze apparatuur zou de kanaalinstelling mogelijk moeten worden gewijzigd.

De deelvragen in dit onderzoek zijn de volgende:

1. Welke typen meters gebruiken de betreffende netbeheerders in de PAMR-band, en in welke aantallen?
2. Per type slimme meter: in hoeverre kan in de praktijk de kanaalinstelling op afstand worden aangepast?
3. Wat is daarvoor nodig, welke risico's zijn er voor de continuïteit van slimme meters en in hoeverre zijn die beheersbaar?

Aanpak

Dit onderzoek is in nauwe samenwerking met technisch specialisten bij de netbeheerders en Utility Connect uitgevoerd. Allereerst is bureauonderzoek uitgevoerd om helder te krijgen hoe het systeem van slimme meters op basis van CDMA in elkaar zit, en welke mogelijkheden er technisch theoretisch gezien zijn om de frequenties te wijzigen. Daarna is onderzocht hoe de relevante meterpopulatie eruitziet, waarbij is gepoogd zoveel mogelijk detailinformatie te verzamelen over de gebruikte modellen en typen CDMA-modems. De verschillende routes voor het wijzigen van de frequentie-instelling zijn besproken en uitgewerkt samen met de technisch specialisten.

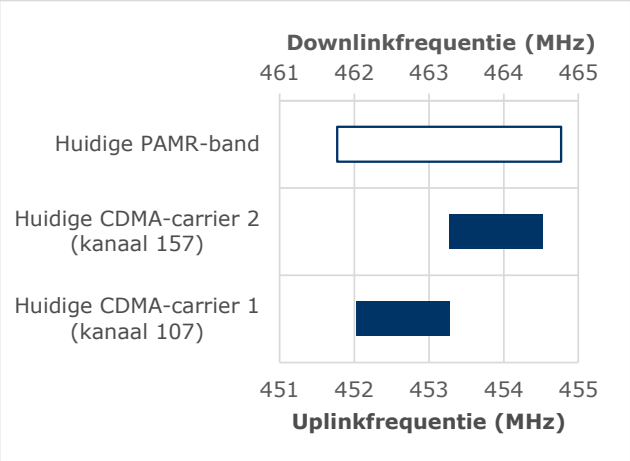
De betrokken netbeheerders (specialisten van Alliander en Stedin) en Utility Connect hebben de mogelijkheid gekregen om op een conceptversie van dit rapport te reageren. De input van beiden is door Dialogic gewogen en meegenomen in het eindrapport.

Leeswijzer

In hoofdstuk 2 geven we een uitleg van de werking van slimme CDMA-meters en de technische achtergrond bij het wijzigen van de gebruikte frequenties. In hoofdstuk 3 geven we onze bevindingen ten aanzien van de situatie bij de Nederlandse netbeheerders. In hoofdstuk 4 geven we tot slot antwoord op de onderzoeksvragen.

2 Technische achtergrond

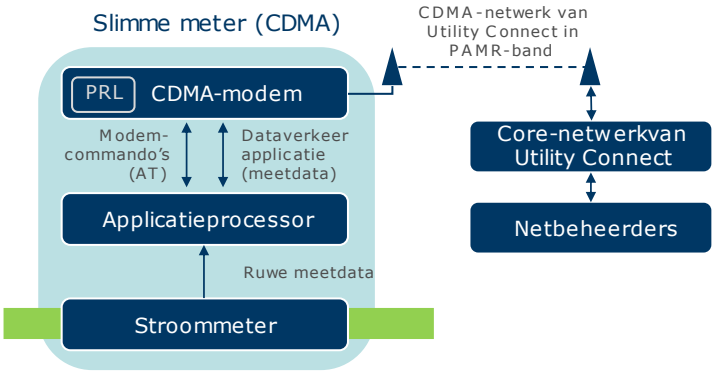
Alliander, Stedin en Westland Infra hebben in Nederland slimme meters uitgerold die communiceren op basis van frequentieruimte in de PAMR-band.[3] Voor het gebruik van deze band beschikt Utility Connect (een joint-venture van Alliander en Stedin, welke het CDMA-netwerk beheert) over een vergunning, waarvan de einddatum 17 november 2024 is. [5] Binnen deze band maakt Utility Connect gebruik van twee CDMA-kanalen (107 en 157 [6]). Figuur 1 toont een schematisch overzicht.



Figuur 1 Huidige frequenties CDMA-netwerk Utility Connect

Werking van slimme CDMA-meters

De slimme meters bevatten een CDMA-communicatiemodule (het 'CDMA-modem') waarmee met het netwerk kan worden gecommuniceerd. In sommige meters is dit een fysiek gescheiden of vervangbare module, in andere modellen is deze geïntegreerd, bijvoorbeeld op of aan de printplaat waar ook de applicatieprocessor van de slimme meter zich bevindt. De software op de applicatieprocessor is verantwoordelijk voor het uitlezen van meetwaarden en het communiceren met de netbeheerder. De applicatiesoftware stuurt hiertoe commando's naar het CDMA-modem. De applicatieprocessor kan ook informatie van het modem ontvangen (zoals informatie over de verbindingsstatus en commando's gericht aan de applicatiesoftware). Figuur 2 toont schematisch deze opzet.



Figuur 2 Schematisch (en zeer vereenvoudigd) overzicht van de werking van een slimme meter op basis van CDMA in de PAMR-band

De CDMA-communicatiemodule verbindt (op basis van instructies van de applicatieprocessor en/of in de fabriek ingeprogrammeerde configuratie) met (in dit geval) het CDMA-netwerk van Utility Connect. De module zoekt daarbij (volgens een gestandaardiseerde procedure, waarvan de precieze implementatie verschilt tussen fabrikanten) naar netwerken binnen de ondersteunde banden. Voordat wordt verbonden met een netwerk wordt gecontroleerd of het netwerk (geïdentificeerd met een *System ID*, een 'netwerknummer' vergelijkbaar met de MCC-MNC bij 3GPP-netwerken) voorkomt op een specifieke lijst (de *Preferred Roaming List*). De PRL kan (indien toegepast) bepalen dat alleen specifieke kanalen mogen worden gebruikt om te verbinden met specifieke netwerken. In dat geval hoeft de meter niet te zoeken naar het netwerk in kanalen waarvan vooraf bekend is dat ze niet door het netwerk worden gebruikt. Hierdoor kan de tijd die het kost om te verbinden met het netwerk ('scantijd') worden verkort.

Noodzaak wijzigen frequenties

EZK heeft zich voorgenomen de PAMR-band onder te verdelen in twee kavels. Kavel A is daarbij bedoeld voor het uitlezen van slimme meters, en strekt van 451,76875-453,26875 MHz (uplink) en 461,76875-463,26875 MHz (downlink). Het tweede kavel betreft 453,26875-454,76875 MHz (uplink) en 463,26875-464,76875 MHz (downlink), en wordt techniekneutraal uitgegeven. [7] Beide kavels zijn 1,5 MHz breed.

[3] 3 MHz gepaard (uplink 451,76875 – 454,76875 MHz en downlink 461,76875 – 464,76875 MHz)

Concreet betekent het voornemen dat de huidige 'bovenste' CDMA-carrier door Utility Connect alleen gebruikt kan blijven worden wanneer Utility Connect een vergunning bemachtigt voor kavel B. Wanneer dit niet het geval is kan alleen kavel A worden gebruikt. De huidige 'onderste' CDMA-carrier valt strikt genomen binnen dit kavel. Echter dient rekening te worden gehouden met interferentie tussen de naastgelegen kavels, en met gebruikers 'onder' en 'boven' de hele PAMR-band. Om deze reden dient de carrier mogelijk te worden 'verplaatst' en is dus ook voor deze carrier een kanaalwijziging nodig. De precieze uitwerking hiervan lijkt ons aan Agentschap Telecom, al dan niet in samenspraak met de toekomstige vergunninghouder(s). In dit rapport beperken we ons tot het onderbouwen van het feit dat de wijziging zeer waarschijnlijk noodzakelijk is.

Omdat het tweede kavel bij voornemen technologieneutraal wordt uitgegeven, is niet exact vast te stellen hoe groot een guard band tussen beide kavels moet zijn. In [3, pp. 28, Tabel 1] gaven we al een overzicht van benodigde guard bands tussen naastgelegen kanalen naar technologie. Het is aannemelijk dat er minimaal ongeveer 225 kHz guard band tussen de CDMA-carrier en de ondergrens van kavel B moet zijn bij een niet-colocated gebruik van kavel B op basis van LTE-M met NB-IoT[4] of 130 kHz wederzijds (dus 260 kHz tussen twee carriers) bij niet-colocated gebruik van kavel B op basis van CDMA[5]. De huidige onderste CDMA-carrier zou vanuit dit perspectief kortom moeten worden verplaatst 'naar onderen' (het alternatief is dat kavel B wordt uitgegeven met beperktere gebruiksmogelijkheden).

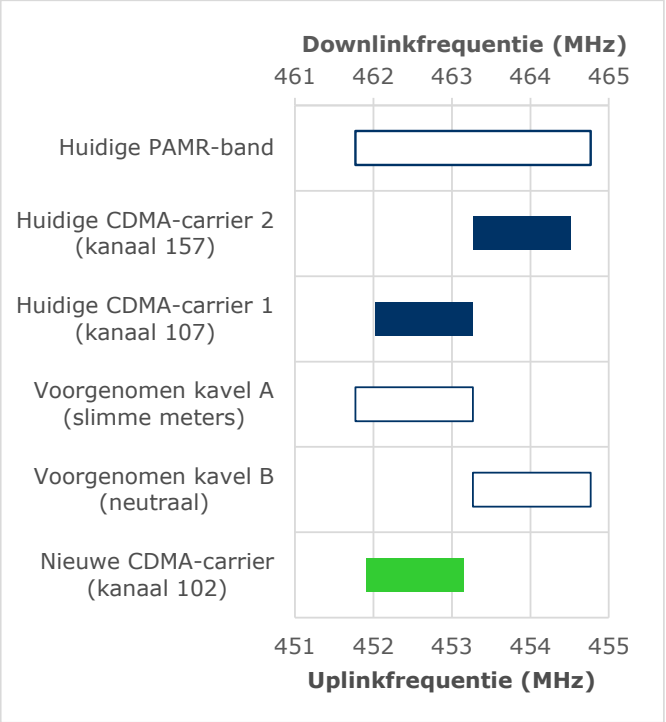
Uiteraard moet ook rekening worden gehouden met gebruikers aan de 'onderkant' van kavel A. Omdat het kavel 1,5 MHz en de CDMA-carrier 1,25 MHz breed is, is slechts 250 kHz aan ruimte over voor guard bands. Onderstaande Tabel 1 toont alle kanalen in CDMA-band 5 block C waarvan de onder- en bovengrenzen binnen kavel A vallen. Afhankelijk van de situatie zou kanaal 101 (106,25 kHz guard aan de onderkant, en 143,75 kHz aan de bovenkant) of kanaal 102 (131,25 aan de onderkant en een krappe 118,75 kHz aan de bovenkant) logisch zijn. De guard bands kunnen tot slot 'smaller' zijn dan hier genoemd wanneer het signaal van de vergunninghouders 'schoner' is dan waarvan in de (3GPP-)aanbevelingen wordt uitgegaan, en/of bij colocated gebruik van kavel B (bijvoorbeeld wanneer de vergunninghouder van kavel B op basis van dezelfde opstelpunten als Utility Connect in kavel A gebruikt CDMA of LTE zou inzetten).

Tabel 1 CDMA-kanalen met onder- en bovengrenzen binnen kavel A (zonder rekening te houden met guard bands)

	Uplink		Downlink	
#	Midden	Van-tot	Midden	Van-tot
96	452,375	451,750-453,000	462,375	461,750-463,000
97	452,400	451,775-453,025	462,400	461,775-463,025
98	452,425	451,800-453,050	462,425	461,800-463,050
99	452,450	451,825-453,075	462,450	461,825-463,075
100	452,475	451,850-453,100	462,475	461,850-463,100
101	452,500	451,875-453,125	462,500	461,875-463,125
102	452,525	451,900-453,150	462,525	461,900-463,150
103	452,550	451,925-453,175	462,550	461,925-463,175
104	452,575	451,950-453,200	462,575	461,950-463,200
105	452,600	451,975-453,225	462,600	461,975-463,225
106	452,625	452,000-453,250	462,625	462,000-463,250
107	452,650	452,025-453,275	462,650	462,025-463,275
108	452,675	452,050-453,300	462,675	462,050-463,300
109	452,700	452,075-453,325	462,700	462,075-463,325
110	452,725	452,100-453,350	462,725	462,100-463,350

[4] Afgaand op 3GPP TR 36.752 moet 385 kHz (edge-to-edge) worden aangehouden tussen een CDMA-carrier en een NB-IoT-carrier wanneer deze laatste onderdeel is van een LTE-M-carrier. Bij een LTE-M-carrier van 1,4 MHz breed zou de afstand 225 kHz moeten zijn (de LTE-carrier bevat de facto een guard band van 180 kHz breed). Wanneer in het kavel 'stand alone' NB-IoT-carriers zouden worden neergezet is de vraag hoe dicht deze tegen de rand van het kavel mogen worden geplaatst. In de basis zal dit vergelijkbaar zijn met de voorgaande situatie, zij het dat er wellicht anders (beter) gefilterd kan worden.

[5] Dit scenario werd al uitgewerkt in [3, 3]



Figuur 3 Voorgenomen verkaveling van de PAMR-band en de noodzaak tot het wijzigen van de frequentie van de onderste CDMA-carrier. De frequentie van de nieuwe carrier (groen) komt 125 kHz lager te liggen dan die van de huidige onderste CDMA-carrier (bij keuze voor CDMA-kanaal 102).

Het op afstand wijzigen van de PRL bij CDMA-terminals

Wanneer de PRL die is ingesteld voor de communicatiemodule in de huidige slimme meters alleen toestaat dat met de bestaande kanalen wordt verbonden met het netwerk van Utility Connect, dan moet deze PRL worden gewijzigd om de meter te kunnen laten verbinden in andere kanalen. Voor het op afstand (via het netwerk) bijwerken van een PRL zijn verschillende methoden, waarvan een aantal zijn gestandaardiseerd en een aantal werken op basis van de applicatiesoftware die de communicatiemodule aanstuurt.

OTA (Over The Air)

De CDMA-standaard voorziet in methoden om 'over the air' een update door te voeren van de PRL (OTA-netwerkfunctie of OTAF). Een van de gestandaardiseerde mechanismen heet OTASP (*Over The Air Service Programming*). [8] De communicatiemodule *vraagt* het netwerk hierbij (op instructie van bijvoorbeeld een modemcommando van de applicatiesoftware) om een nieuwe PRL. Een gebruiker van een CDMA-telefoon kan deze procedure starten door een specifieke code te 'bellen'.[6] Om van deze route gebruik te maken moet de software van de applicatieprocessor een functie bevatten om deze instructie te geven. Daarnaast moet de applicatieprocessor beschikken over een interface om de communicatiemodule instructies te geven (en niet alleen om data te versturen).

Een ander mechanisme is OTAPA (*Over The Air Parameter Administration;* [8, pp. 3-4, 3.2.2]). De communicatiemodule gaat hierbij de PRL bijwerken na ontvangst van een specifiek verzoek daartoe van het netwerk. Dit verzoek bestaat uit een oproep gericht aan het modem waaraan een specifieke vlag is toegevoegd.

AT-commando's

Met AT-commando's (ook bekend als de *Hayes command set*) kunnen modems worden aangestuurd door applicatiesoftware. Zo kan het modem worden geïnstrueerd met een bepaald netwerk verbinding te maken, de verbinding te verbreken, een gesprek of datasessie op te zetten, et cetera. Het modem kan eveneens rapporteren over de huidige status (of er verbinding is, signaalsterkte, et cetera). Er is geen algemene standaard voor AT-commando's; wel is er een 3GPP-standaard voor AT-commando's voor 3GPP-terminals [9]. De 3GPP2-standaard specificeert geen AT-commando voor het aanpassen van de PRL. Naast de gestandaardiseerde en 'well known' AT-commando's ondersteunen modems vaak echter ook enkele niet-gestandaardiseerde, fabrikant-specifieke commando's. Zo ondersteunt de LISA C200-module van u-Blox (voor zover wij weten niet toegepast in Nederlandse slimme meters) het commando "AT+PRL=2" om een OTA PRL-update te initiëren. [10, pp. 58-59].

[6] Zie [8], 3.2.1 "User initiated procedure". Het te bellen nummer is *FC*XX, waarbij 'FC' (feature code) gelijk is aan '228' en 'XX' een indicatie van de band. Onduidelijk is wat deze code is voor de 450-band.

Aanpassing van parameters via OTAPA wordt beperkt door beveiligingsmaatregelen wanneer het modem in de 'locked'-toestand is gebracht die bepalen welke parameters mogen worden gewijzigd.[7]Voordat een update via OTAPA wordt toegepast wordt deze gecontroleerd aan de hand van een digitale handtekening. Het is dus nodig dat men beschikt over de benodigde digitale sleutels. Bij deze methode is verder geen betrokkenheid van de applicatiesoftware nodig.

De standaard stelt als uitgangspunt dat OTAPA ingeschakeld dient te zijn op een modem. Daarnaast wordt aanbevolen een fabrikant-specifiek commando te implementeren waarmee OTAPA kan worden uitgeschakeld. [8, pp. 3-4]

Voor OTA is aan de netwerkzijde een 'OTA-functie' (OTAF) benodigd. Deze is niet vereist wanneer geen OTA wordt gebruikt en daarom niet per definitie aanwezig in een CDMA-netwerk.

Update PRL via het netwerk middels update applicatiesoftware

De applicatiesoftware kan een PRL-bestand 'uploaden' naar de communicatiemodule. Om via deze weg de PRL te updaten dient de applicatiesoftware te worden bijgewerkt zodat deze (bijvoorbeeld bij de eerste keer opstarten) een PRL-update uitvoert. De modemfirmware dient hiervoor een interface of commando beschikbaar te stellen.

Een voorbeeld van een modem dat een dergelijk commando wel ondersteunt, is de u-Blox LISA C200. Dit modem accepteert het commando "`AT+UPRLWRITE:`" waarmee een PRL-bestand kan worden geschreven naar de permanente opslag van het modem. [10, pp. 64-65]. Voor zover bekend wordt deze module niet gebruikt in Nederlandse slimme CDMA-meters. Verderop zal blijken dat de gebruikte communicatiemodules deze commando's waarschijnlijk niet ondersteunen.

Update modemfirmware via applicatiesoftware

De applicatiesoftware zou, als het daarvoor over de juiste toegang beschikt, de firmware van de communicatiemodule kunnen updaten. Hiervoor dient waarschijnlijk de applicatiesoftware eerst te worden geüpdatet, zodat deze beschikt over de nieuwe firmware en de instructies om deze update uit te voeren. De bijgewerkte modemfirmware bevat de nieuwe PRL bevat de ondersteuning voor het OTA bijwerken van de PRL, of bevat de ondersteuning voor het bijwerken via de applicatiesoftware. In de laatste twee gevallen is de update dus een 'tweetrapsraket'.

Fysieke vervanging

Een laatste mogelijkheid is het aanpassen van de PRL-instelling op locatie, bijvoorbeeld door de communicatiemodule fysiek te vervangen en/of via een kabel opnieuw te configureren. Gezien de aantallen is het aannemelijk dat dit een zeer kostbare operatie is. Door beveiligingen op de meter zijn dit soort aanpassingen niet triviaal en ligt vervanging van de meter bij monde van de netbeheerders meer voor de hand van aanpassing van een geïnstalleerde meter. [3] Bij vervanging van een stroommeter op basis van de DSMR 4-standaard dient ook de gasmeter vervangen te worden.

[7] Dit mechanisme heet SPASM (*Subscriber Parameter Administration Security Mechanism*) en de bedoelde staten zijn SP_LOCK_STATE en NAM_LOCK_STATE. Wanneer SP_LOCK_STATE=1 zijn de parameters vergrendeld. [8, pp. 1-5]

3 Bevindingen

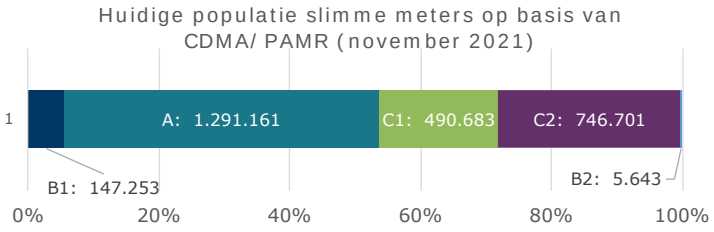
Meterpopulatie

De grootschalige uitrol van slimme meters begon in Nederland in 2015. Op dit moment zijn er volgens de netbeheerders 2,68 miljoen slimme meters op basis van CDMA-connectiviteit uitgerold (door Alliander, Stedin en Westland Infra).

De levensduur van de eerste generatie CDMA-meters (op basis van DSMR 4.3, uitgerold tussen 2015 en 2017) is door de netbeheerders gesteld op (ten minste) 15 jaar. Dat zou betekenen dat deze slimme meters nog tot minimaal 2033 in gebruik zullen zijn. [3] Het merendeel van de nu actieve meters werd tussen 2018 en 2020 uitgerold, en voor deze groep geldt een levensduur tot 2035. Utility Connect houdt rekening met beschikbaarheid van het netwerk tot en met ten minste 2034.

Tabel 2 geeft een overzicht van de huidige populatie slimme meters die werken op basis van CDMA. De netbeheerders geven aan dat deze meters min of meer willekeurig (per straat/wijk) zijn uitgerold (het is dus niet zo dat in een bepaalde regio alleen bepaalde meters worden gebruikt).

Tabel 2 Overzicht huidige CDMA-meterpopulatie (bron: netbeheerders)



Merk/type	Aantal
A	1.291.161
B1	147.253
B2	5.643
C1	490.683
C2	746.701
Totaal	**2.681.441**

Noot: de namen en modelnummers van de meters doen niet terzake voor de onderbouwing van de in dit rapport gepresenteerde conclusies. De namen zijn gepseudonimiseerd op verzoek van de netbeheerders, die aangeven dat het noemen van de namen de relatie met de fabrikanten kan verstoren. In een (vertrouwelijke) bijlage is een lijst opgenomen met fabrikant/type meter en bijbehorende letter.

Voor ieder metertype bestaan verschillende subtypen (voor verschillende soorten elektriciteitsaansluitingen) met ieder eigen varianten van de metersoftware (gebaseerd op dezelfde hoofdversie).

Metertype A

De PRL in deze meters is ingesteld op de huidige CDMA-kanalen en 'System ID' van het netwerk van Utility Connect.

Metertype B1

De PRL in deze meters is ingesteld op de huidige CDMA-kanalen en 'System ID' van het netwerk van Utility Connect. Het is aannemelijk dat in een kleine subset oudere B-meters ook nog een ouder CDMA-kanaal van KPN voorkomt in de PRL. Dit kanaal valt buiten de huidige PAMR-band en kan dus geen rol van betekenis spelen in de voorgenomen migratie.

Metertype B2

Dit metertype is de opvolger van type B1, op basis van de meer recente SMR 5-specificatie. Van dit metertype zijn op dit moment nog slechts 5.643 exemplaren uitgerold.

De PRL in deze meters is ingesteld op de huidige CDMA-kanalen en 'System ID' van het netwerk van Utility Connect.

Metertype C1

De PRL in deze meters is ingesteld op de huidige CDMA-kanalen en 'System ID' van het netwerk van Utility Connect.

Metertype C2

De PRL in deze meters is ingesteld op de huidige CDMA-kanalen en 'System ID' van het netwerk van Utility Connect. Dit type meter lijkt technisch gezien sterk op type C1.

Mogelijkheden voor het wijzigen van de kanaalinstelling

Geen van de meters, behalve waarschijnlijk de meters van type B, ondersteunen OTA. Vanuit het netwerk is het realiseren van OTA eveneens nagenoeg onmogelijk. De netbeheerders hebben dan ook ingezet op het (door de fabrikant laten) ontwikkelen van firmware-updates die een nieuwe PRL bevatten (afhankelijk van de gebruikte modemmodule zal de update vervolgens via een AT-commando, update van de modemsoftware en/of update van een PRL-file verlopen).

Tabel 3 toont het overzicht van de populatie CDMA-meters en de status (medio maart 2022) van ontwikkeling van deze software-update.

Tabel 3 Overzicht populatie CDMA-meters en oplossingsrichting voor wijzigen kanaalinstelling (medio maart 2022)

Merk/type	Aantal	Status (begin maart 2022)
A	1.291k	De fabrikant heeft van de modemleverancier een nieuwe versie van de modemfirmware ontvangen waarin de PRL gewijzigd is. Het is echter nog niet mogelijk gebleken deze modemfirmware op afstand bij te werken. De fabrikant is in afwachting van een 'delta image' van de modemfabrikant waarmee de firmware dan wel zou kunnen worden bijgewerkt via een software-update. De fabrikant heeft hiervoor geen tijdspad aangegeven. De netbeheerders zijn voortdurend in overleg met de fabrikant om te zorgen dat de update wordt gerealiseerd.
B1	147k	Voor dit metertype is een software-update ontwikkeld die op afstand kan worden uitgevoerd, en die de kanaalinstelling wijzigt. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.
B2	6k	Voor dit metertype is een software-update ontwikkeld die op afstand kan worden uitgevoerd, en die de kanaalinstelling wijzigt. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.
C1	491k	Voor dit metertype is een software-update ontwikkeld die op afstand kan worden uitgevoerd, en die de kanaalinstelling wijzigt. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.
C2	747k	Voor dit metertype is een software-update ontwikkeld die op afstand kan worden uitgevoerd, en die de kanaalinstelling wijzigt. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.

Metertype A

De fabrikant geeft aan dat haar meters geen ondersteuning bevatten voor het bijwerken van de PRL via OTA, noch dat er een andere mogelijkheid is om de PRL op afstand bij te werken. Later heeft de fabrikant aangegeven dat een route via een firmware-update mogelijk zou zijn.

De netbeheerders wachten op moment van schrijven, na meermaals aandringen, nog altijd op een software-update van de fabrikant. De fabrikant gaf eerder aan dat het medewerking van de leverancier van de modemmodule (Sierra Wireless) nodig had; zij zouden wachten op informatie van de modemleverancier (Qualcomm). Eind februari werd een update voor de modemfirmware opgeleverd, waarin de PRL is gewijzigd. Deze update kan echter niet op afstand worden geïnstalleerd. De meterfabrikant is nu in afwachting van een 'delta image' van de modemfabrikant. Met dit 'delta image' zou de firmware van het modem op afstand kunnen worden bijgewerkt via een software-update. De fabrikant heeft hiervoor geen tijdspad aangegeven. Na het opleveren van een software-update moet deze uiteraard nog getest worden.

Metertype B1

Voor deze meter wordt dezelfde oplossing voorzien als voor de nieuwere B2-meter (zie verderop). Voor deze meter was de fabrikant in eerste instantie nog

op zoek naar de nodige informatie van de modemleverancier. De netbeheerders hebben enkele meters opgestuurd naar de fabrikant ten behoeve van het ontwikkelen van de update. Inmiddels is een software-update opgeleverd, welke volledig is getest en akkoord bevonden door de netbeheerders/Utility Connect.

Metertype B2

De fabrikant had in eerste instantie aan de netbeheerders aangegeven dat de meters een OTA-update van de PRL ondersteunen. Hiertoe zou een "configuratie-SMS" dienen te worden verstuurd naar de meter (de bedoelde procedure lijkt dan ook OTASP te zijn).

De fabrikant heeft later aangegeven dat het bijwerken van de PRL mogelijk is via een software-update van de meter, die de firmware van de modemmodule bijwerkt.

De netbeheerders hebben voor de B1-meter een updateprocedure en een nieuwe versie van de software ontvangen. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.

Metertype C1

De fabrikant heeft voor deze meter een software-update opgeleverd. De update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.

Metertype C2

De netbeheerders geven aan dat de software van dit type (voor zover zij kunnen beoordelen) sterk lijkt op die van type C1. Voor dit meterype is dan ook kort na het slagen van de test van de update voor de C1-meter eveneens een update opgeleverd door de meterfabrikant. Deze update is volledig getest en akkoord bevonden door de netbeheerders/Utility Connect.

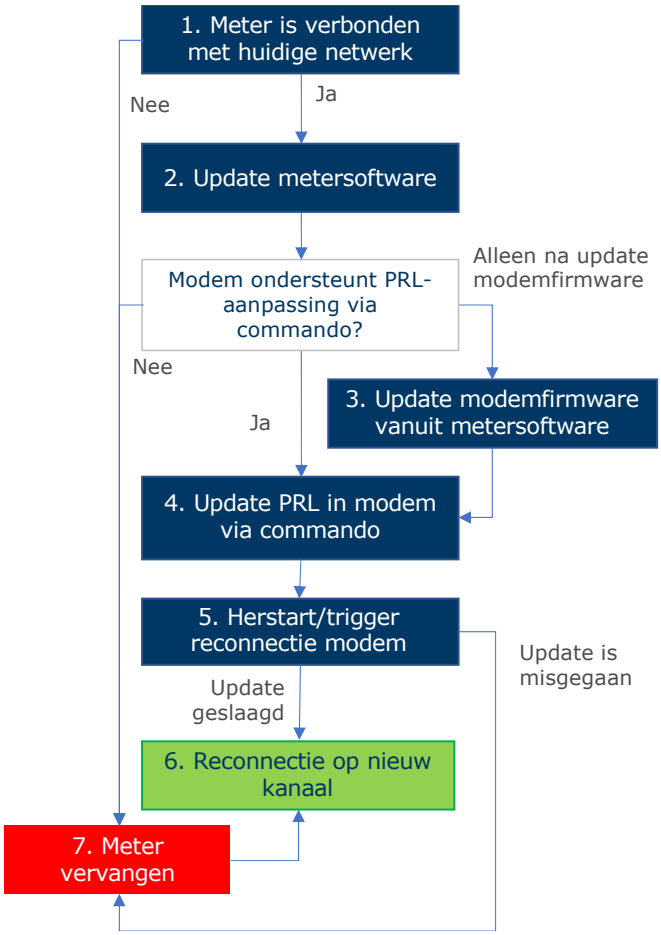
Haalbaarheid van een OTA-update aan de netwerkzijde

Voor de OTA-procedure is aan netwerkzijde primair een zogenaamde 'OTA-functie' (OTAF) nodig. Deze functie omvat primair het op een veilige manier 'uitreiken' van nieuwe instellingen aan terminals die daarom vragen. De OTA-functie wordt vervuld door een 'OTA-server' welke gekoppeld is aan het HLR (Home Location Register; de database met alle gegevens over aangesloten terminals).

Utility Connect geeft (op basis van informatie van onder andere de leverancier van haar netwerkkern) aan dat OTA niet kán worden ondersteund op haar netwerk, en heeft dit aan de onderzoekers voldoende aannemelijk gemaakt. Utility Connect geeft aan dat de onderliggende redenen hiervoor bedrijfsvertrouwelijk zijn. Op verzoek van Utility Connect, en rekening houdend met het feit dat de netbeheerders nu uitsluitend oplossingsroutes zónder OTA uitwerken, is de argumentatie bij dit punt niet opgenomen in de hoofdtekst van dit rapport, maar in de (vertrouwelijke) Bijlage 2.

Mogelijke risico's van een frequentiewijziging

Figuur 4 toont het stappenplan dat moet worden doorlopen om de huidige populatie CDMA-meters te connecteren op een nieuw, gewijzigd CDMA-kanaal. Bij iedere actie (blauwe blokken) kunnen zich *risico's* voordoen. Een risico heeft (uiteindelijk) altijd het gevolg dat een meter niet meer kan worden geconnecteerd via het nieuwe kanaal, en dus fysiek moet worden vervangen. Naast de risico's zijn er *onzekerheden*: het is op dit moment niet duidelijk welke 'afslagen' in de figuur kunnen worden genomen.



Figuur 4 Stappenplan voor het aanpassen van de kanaalinstelling bij de huidige populatie CDMA-meters

Risico's per stap

1. Meter is verbonden met het huidige netwerk

Hoewel deze actie triviaal klinkt (de huidige meters *zijn* verbonden met het huidige netwerk) is het toch relevant om deze te benoemen. Het is namelijk aannemelijk dat er meters zullen zijn die op moment van uitvoeren van de stappen niet zijn aangesloten (vanwege een instabiele verbinding of om andere redenen). Wanneer de wijziging is voltooid, en ook de tweede carrier is uitgeschakeld, zijn deze meters niet later alsnog op afstand aan te passen, en dienen ze fysiek te worden vervangen.

2. Update metersoftware

De netbeheerders geven aan dat iedere software-update van een slimme meter in de praktijk leidt tot uitval van een klein percentage (±0,5%, omgerekend ongeveer 13.500 meters [3]) van de meters. De oorzaak hiervan moet worden gezocht in fouten tijdens het updateproces (de update wordt onjuist weggeschreven, de stroom werd onderbroken tijdens de update, een bestaand defect wordt zichtbaar omdat de meter herstart, et cetera). Dergelijke updates worden overigens nu al sporadisch (hooguit enkele keren per jaar) uitgevoerd; uitval hierdoor is dus een gekend risico.

3. Update modemsoftware vanuit metersoftware

De netbeheerders geven aan dat een update om de modemfirmware bij te werken waarschijnlijk risicovoller is. Er is niet eerder een update van de modemfirmware uitgevoerd. Een dergelijke update is groter dan de updates die tot nu toe zijn doorgevoerd. Daarnaast is het updateproces complexer (de software op de meter moet worden geüpdatet, waarna deze software de update op het modem uitvoert). De redenen die worden aangevoerd bij het hogere risico zijn technisch gezien begrijpelijk.

Een te verwachten uitvalspercentage is lastig te bepalen. De netbeheerders schatten de kans op uitval op maximaal 5-10% (wat zou neerkomen op tussen de 134.000 en 268.000 meters), waarbij de netbeheerders aangeven dat deze schatting niet is onderbouwd. Vanuit ons perspectief lijkt het realistisch(er) om uit te gaan van (maximaal) een verdubbeling van het reguliere uitvalspercentage (±1%, wat zou neerkomen op een uitval van ±27.000 meters). Nadere tests zullen moeten uitwijzen hoe hoog het uitvalpercentage in de praktijk zal zijn.

4. Update PRL in modem via commando

Wanneer het modem een commando ondersteunt waarmee de PRL kan worden aangepast, is het aanpassen zelf op zich geen risicovolle actie. Uiteraard bestaat er ook in deze stap een kleine kans dat de actie misgaat (al is het juist wegschrijven van de PRL achteraf door de software te verifiëren en zou dit bij een fout kunnen worden herhaald) door bijvoorbeeld een communicatiefout of defect geheugen.

Deze stap kan worden overgeslagen als de modemfirmware zelf de nieuwe PRL bevat.

6. Herstart/trigger reconnectie

Nadat de PRL is bijgewerkt is het mogelijk dat het modem in de slimme meter niet direct zal proberen te verbinden volgens het nieuwe regime. Dit is afhankelijk van de modemsoftware. Wanneer het modem niet direct naar het netwerk begint te zoeken na het wijzigen van de PRL (bijvoorbeeld omdat het de PRL alleen bij het opstarten van het modem inleest), is het nodig om een dergelijke scan te

'triggeren' (bijvoorbeeld door de CDMA-carrier even uit en aan te zetten, de modemmodule en/of de meter te herstarten, het modem een resetcommando te geven, et cetera).

Het maakt niet uit als een van de in PRL gespecificeerde kanalen voor iets anders (bijvoorbeeld LTE) wordt ingezet. Het modem zal (volgens de standaard) pas proberen aan te melden (en dus zenden) wanneer deze een CDMA-signaal heeft herkend in een van de banden.

Mocht een PRL-update falen, dan blijft de eerder ingestelde PRL van kracht.[8] Het is dan dus mogelijk om nogmaals een PRL-update te proberen,[9] zolang het netwerk nog actief is in de 'oude' kanalen. Het uitschakelen van het 'oude' kanaal kan meters met de nieuwe PRL ertoe dwingen om te verbinden met het nieuwe kanaal.

De risico's die deze actie oplevert zijn relatief klein (het netwerk moet immers ook in een situatie van bijvoorbeeld stroomuitval kunnen herstellen), al zal de uitval als gevolg van de andere acties op dit moment daadwerkelijk plaatsvinden. Daarnaast zijn er ook andere gebruikers van het CDMA-netwerk, die uiteraard hinder zullen ondervinden wanneer de carriers worden uitgeschakeld.

6. Reconnectie op nieuw kanaal

Alles wijst erop dat de CDMA-meters technisch gezien zonder problemen zouden moeten kunnen functioneren op andere kanalen binnen de huidige band. Satimo heeft dit in opdracht van de netbeheerders onderzocht, en onder andere gekeken naar de signaalkwaliteit. Het onderzoek werd uitgevoerd met de relevante modellen, in een speciale 'testmodus' geplaatste of zelfs fysiek aangepaste meters, waarin de kanaalinstelling kon worden gewijzigd. De test is uitgevoerd in een gecontroleerde omgeving (en dus niet met het netwerk van Utility Connect).

Het wijzigen van de kanalen zou afhankelijk van de locatie in theorie kunnen leiden tot te lage signaalkwaliteit, waardoor sommige meters buiten bereik van het netwerk kunnen vallen. Het onderzoek van Satimo heeft de netbeheerders echter doen concluderen dat de radioperformance in alle gevallen bleef voldoen aan de door de netbeheerders gestelde eisen. Interferentie van andere gebruikers is daarbij overigens buiten beschouwing gelaten.

Daarnaast speelt het feit dat hetzelfde aantal meters in de voorziene situatie gebruik moet maken van één carrier, waar deze op dit moment worden verdeeld over twee carriers. Dit leidt in sommige gebieden wellicht tot een capaciteitstekort. In [3] werd al een korte analyse getoond van de locaties waar deze capaciteitsissues voornamelijk zouden kunnen gaan spelen.

In theorie zijn beide problemen op te lossen door het netwerk te verdichten.

Herhaling van de stappen

In de huidige meters is de PRL beperkt tot de twee kanalen die op dit moment worden gebruikt. De reden hiervoor is dat de procedure waarbij de meter zoekt naar het juiste kanaal zo kort mogelijk duurt (en de meter bij verlies van de verbinding dus ook snel weer verbonden is). Een PRL met meer toegestane kanalen leidt zo bezien tot meer stabiliteit. Uiteraard kan de PRL na migratie door herhaling van de procedure weer worden 'ingekort'.

[8] Ten minste, wanneer de update van de PRL op een robuuste manier is geïmplementeerd. Zo zou de bijgewerkte PRL achteraf moeten worden geverifieerd en zou de update opnieuw moeten worden gestart wanneer blijkt dat de PRL tijdens de update corrupt is geraakt.

[9] Een complicatie is dat een slimme meter om beveiligingsredenen geen update accepteert waarvan het versienummer ouder of gelijk is aan de nu geïnstalleerde versie. Voor een tweede poging is dus een nieuwe versie nodig. Het ligt daarom voor de hand om in de software zélf een 'retry'-mechanisme op te nemen.

4 Conclusie

Beantwoording onderzoeksvraag

In hoeverre kunnen netbeheerders de kanaalinstelling in de slimme meters op afstand aanpassen?

De slimme meters op basis van CDMA zijn af-fabriek ingesteld om alleen te verbinden met het CDMA-netwerk van Utility Connect in de nu gebruikte kanalen. Er is op voorhand niet voorzien in een mogelijkheid om deze kanaalinstelling van slimme meters op basis van CDMA op afstand te wijzigen. Het CDMA-netwerk van Utility Connect kán geen ondersteuning bieden voor de gestandaardiseerde methoden voor een dergelijke update (OTA-update van PRL). De enige andere mogelijke route voor het op afstand aanpassen van de kanaalinstelling is dan ook het uitrollen van een update van de software op de slimme CDMA-meters. Deze update kan de kanaalinstelling in het modem van de meter wijzigen met een commando. Afhankelijk van het type meter dient vooraf ook een update van de modemfirmware te worden uitgevoerd.

Het aanpassen van de kanaalinstelling van de betreffende CDMA-meters kent een risico op uitval van (verwachting onderzoekers) ongeveer 1% (circa 27.000 meters).

Beantwoording deelvragen

Welke typen meters gebruiken de betreffende netbeheerders in de PAMR-band, en in welke aantallen?

Tabel 4 toont de populatie van slimme meters die de netbeheerders (Alliander, Stedin en Westland Infra) op dit moment gebruiken, en die gebruik maken van CDMA in de PAMR-band voor communicatie. De letters verwijzen naar fabrikanten en de cijfers naar verschillende metertypen van de betreffende fabrikant.

In totaal gaat het om ongeveer 2,68 miljoen meters die vanaf 2015 en hoofdzakelijk tussen 2018-2020 zijn geplaatst, met een beoogde levensduur tot 2035. Het gaat om vijf typen meters van drie fabrikanten, waarvan drie typen het meest voorkomen, en één type nauwelijks.

Tabel 4 Overzicht aantallen per type meter

Merk/type	Aantal
A	1.291.161
B1	147.253
B2	5.643
C1	490.683
C2	746.701
Totaal	**2.681.441**

Per type slimme meter: in hoeverre kan in de praktijk de kanaalinstelling op afstand worden aangepast?

Geen van de typen slimme CDMA-meters ondersteunt op dit moment het op afstand wijzigen van de kanaalinstelling.

Om de kanaalinstelling desondanks op afstand te kunnen wijzigen is een update van de metersoftware nodig. Een dergelijke update kan ofwel (1) de modemfirmware bijwerken zodat deze een nieuwe PRL bevat, (2) een commando sturen naar het modem om de PRL bij te werken (3) de modemfirmware bijwerken zodat deze aanpassing van de PRL via een commando ondersteunt, en vervolgens het commando sturen. Bij (1) en (3) moet dus ook de modemfirmware worden bijgewerkt.

Type	Status (medio maart 2022)
A	Wacht op uitbrengen update door fabrikant, die wacht op 'delta'-firmware-update van de modemfabrikant.
B1	Update opgeleverd en met succes getest.
B2	Update opgeleverd en met succes getest.
C1	Update opgeleverd en met succes getest.
C2	Update opgeleverd en met succes getest.

Wat is daarvoor nodig, welke risico's zijn er voor de continuïteit van slimme meters en in hoeverre zijn die beheersbaar?

Figuur 4 toont op hoofdlijnen de stappen die moeten worden doorlopen om de kanaalinstelling van slimme CDMA-meters te wijzigen (langs verschillende routes). Iedere stap in deze procedure kan risico's met zich meebrengen. Het primaire risico is dat een meter niet meer opnieuw verbindt met het netwerk, omdat de update van de metersoftware en/of de

modemfirmware is misgegaan (of een bestaand defect zichtbaar wordt wanneer de meter vanwege de update wordt herstart).

Een reguliere software-update leidt tot ongeveer 0,5% uitval. De hier benodigde update is wellicht iets risicovoller, omdat bij sommige metertypen ook de modemfirmware wordt geüpdatet. Het wijzigen van de kanaalinstelling op zichzelf leidt (afgaand op de resultaten van Satimo) niet tot (aanvullende) radiotechnische problemen die tot uitval zouden kunnen leiden.

Een te verwachten uitvalspercentage is lastig te geven, maar schatten de onderzoekers op maximaal het dubbele van een reguliere update (ergo 1%). In absolute termen gaat het dan om uitval van ongeveer 27.000 meters. De netbeheerders zijn pessimistischer en houden rekening met maximaal 5-10%. Hoewel deze percentages niet nader onderbouwd (en wat ons betreft niet realistisch) zijn, delen we wel het argument van de netbeheerders dat een kleine verhoging van het percentage in absolute zin een grote impact heeft, vanwege de hoge aantallen meters. Praktijktests en een geleidelijke uitrolstrategie zullen moeten uitwijzen wat het uitvalpercentage in de praktijk zal zijn. Een uitgevallen meter leidt overigens niet direct tot uitval van de stroomvoorziening bij de betreffende aansluiting. De netbeheerder moet de meter wel fysiek op locatie vervangen.

Het wijzigen van de kanalen (specifiek het gebruiken van één in plaats van twee uitwisselbare kanalen) kan tot slot leiden tot plaatselijk capaciteitstekort en incidenteel een slechter signaal, waarvoor het netwerk zou moeten worden aangepast (verdicht), zoals al beschreven in [3].

Voor alle behalve één type meter is inmiddels een software-update ontwikkeld waarmee de kanaalinstelling op afstand kan worden gewijzigd, en is deze update met succes getest. De netbeheerders hebben hiermee de mogelijkheid gekregen de kanaalinstelling voor deze meters op afstand te wijzigen. Voor het resterende metertype, in aantal de meest voorkomende, is weliswaar een nieuwe versie van de modemfirmware ontwikkeld waarin de kanaalinstelling kan worden gewijzigd, maar is het nog niet gelukt deze op afstand bij te werken via een software-update. Een tijdspad voor het opleveren van een werkende software-update is niet afgegeven. Het is niet met zekerheid te zeggen of deze software-update uiteindelijk kan worden gerealiseerd voor dit metertype, of dat er technische redenen zijn die dit niet mogelijk maken.

Verwijzingen

[1] Ministerie van Economische Zaken (2005). *Vergunning voor gebruik frequentieruimte t.b.v. Public Access Mobile Radio (PAMR)* [zoek.officielebekendmakingen.nl] Den Haag,

[2] Ministerie van Economische Zaken en Klimaat (2018). *Besluit verlengbaarheid PAMR-vergunning 2018* [zoek.officielebekendmakingen.nl] vol. 2018,

[3] Dialogic, van der Vorst, T., van Rees, J., en Hanswijk, M. (2020). *Mogelijkheden voor het PAMR-spectrum in relatie tot continuïteit van slimme meters* [www.rijksoverheid.nl]

[4] Westland Infra, Stedin en Alliander (2021). *Consultatiereactie beleidsvoornemen PAMR-band 450-470 MHz-spectrum* [internetconsultatie.nl]

[5] Agentschap Telecom (2019). *Geconsolideerde versie van de PAMR-vergunning (Utility Connect B.V.) juli 2019* [www.internetconsultatie.nl] Groningen: Agentschap Telecom.

[6] 3GPP2 (2006). *Band Class Specification for cdma2000 Spread Spectrum Systems.Revision B.* [www.3gpp2.org]

[7] Ministerie van Economische Zaken en Klimaat (2020). *Beleidsvoornemen toekomstig gebruik van de PAMR-band (2 x 3 MHz) in het 450–470 MHz spectrum* [www.internetconsultatie.nl] Den Haag,

[8] 3GPP2 (2008). *Over-The-Air Service Provisioning of Mobile Stations in Spread Spectrum Systems* [www.3gpp2.org]

[9] 3GPP, TSG Terminals (2003). *AT command set for User Equipment (UE)*

[10] u-Blox (2014). *LISA-C200 and FW75-C200 CDMA 1XRTT Cellular Modules. AT Commands Manual* [www.u-blox.com]

[11] ZTE. *Document for updation of PRL in OTA/manually created MIN/MDN* [cupdf.com]

[12] Telit (2015). *AT Commands Reference Guide For CL865 series* [www.telit.com]

[13] Open Mobile Alliance. *OMA Device Management Overview* [technical.openmobilealliance.org]