Echelon type 83331-3IAAD ”hack”

Hvem er vi?

Graves Kilsgaard
Uddannet Datamatiker fra IT akademiet i Skive i 1995.
Startede som systemadministrator, men har de sidste ca. 20 år gået over til primært at være arkitekt og systemudvikler, med speciale inden for MS SQL, Business Intelligence, integrationer og Microsofts ERP (AX / NAV / BC).

Arbejder i dag som cloudarkitekt og systemudvikler hos KMC a.m.b.a. i Brande.

Interessen for elektronik og 3D print steg da Arduino og Raspberry pi kom på markedet, hvorved det blev nemt og billigt at lave små DIY-projekter. Siden 2017 har nørderiet foregået sammen med Gert Lynge.

https://www.linkedin.com/in/kilsgaard/

graves@dabbler.dk

Gert Lynge

Uddannet Datamatiker fra IT akademiet i Skive i 1995.

Har ejet egen it-butik, været teknisk direktør for internetudbydere og arbejdet en del år som intern udvikler af økonomisystemer.

I de seneste år har Gert arbejdet som konsulent og udvikler indenfor økonomisystem (ERP) - branchen.

Gert er i dag chefudvikler i Herningvirksomheden SIMTEQ A/S (www.simteq.com), og laver løsninger i økonomisystemet Microsoft Dynamics 365 Business Central (tidl. NAV/Navision).

Ud over en smule elektronikundervisning som ung, har Gert fusket med elektronik nogle timer ca. en gang om ugen siden 2017 og sammen med Graves Kilsgaard.

https://www.linkedin.com/in/gertlynge/

gert@dabbler.dk

Disclaimer

Samme ansvarsfraskrivelse som på vores blog: www.dabbler.dk

We are friends dabbling with electronics, software and .... stuff, and need a place to document whatever we learn.

We decided that if we share our questionable knowledge on this blog, others might find it useful or simply blow themselves up because we got it totally wrong :-)

Most information on this blog is probably stolen from somewhere else (sorry), misunderstood or simply plain wrong - so if you use it, it is your own risk and expense.

BEWARE - YOU HAVE BEEN WARNED!!! :-)

Enjoy!

Før Sommerhack 2020

- Hvad har andre forsøgt og hvad har vi forsøgt?
  Se evt. Poul-Henning Kamps indlæg og andres kommentarer på: https://ing.dk/blog/hvilken-elmaaler-har-du-120890

  - Tælle ”pulser” fra lysdiode /
    tælle omgange på drejeskive
  - Måling v.h.a. af induktion – se fx SCT013”non-invasive AC current sensor” på ebay.com
  - Løsning med pulsende elektrisk signal
  - Kommunikation via IR-øjet

Sommerhack 2020

To foredrag fik os ”tændt” på vores gamle skuffeprojekt:

- Data fra fjernaflæste elmålere – Christian Holmer Henriksen, N1 (https://n1.dk/)
- Hvor sikker er vores ”smarte” el-målere egentligt – Thomas Ljungberg Kristensen, WelcomeSecurity (https://www.welcomesecurity.net/)

PS: For dem der deltog - det var os der vist fik nævnt ”API” en enkelt gang eller to ☺

Sommerhack 2021

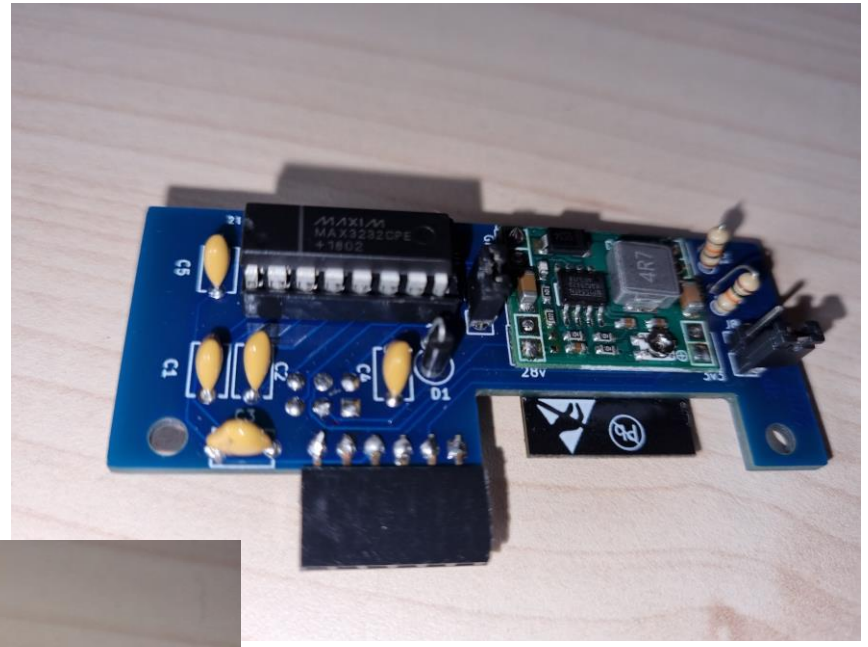
Nu har vi en fungerende prototype:

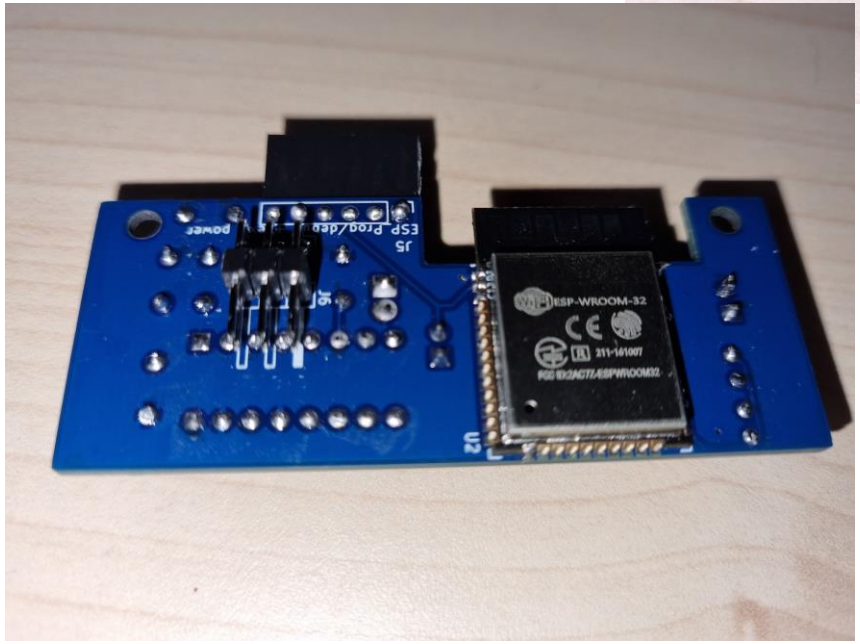
- Multi-purpose Expansion Port (MEP)
  NB: MEP findes også i andre NES/Echelon måleren end type 83331-3IAAD. Nogle nyere har endda 2 MEP interfaces.

- Passer i Echelon målerens MEP-”skuffe”

- ESP32 (WIFI)

- Strømforsynes fra elmåleren
  1watt er tilsyneladende lige nøjagtigt nok…





Processen

På opfordring fra Thomas kontaktede vi Energi Midt:

- Norlys (Energi Midt) henviser til N1
- N1 nægter adgang til IR port – krypteret og nøglerne MÅ ikke udleveres
- N1 oplyser vi skal købe et Izar / M-Bus print, men kan ikke oplyse hvor det kan købes – men at det er udviklet af Develco (https://develco.dk/)
- Vi finder en PDF og kan se det er ikke helt korrekt – det Develco har lavet er et ZigBee / MEP print (ikke Izar / M-Bus som er andre standarder)
  https://www.yumpu.com/en/document/view/10203117/08-peter-k-hansen-develco-specification-mep-esna
  (alternativt: https://www.dabbler.dk/wp-content/uploads/2021/08/08-Peter-K.-Hansen-Develco-Specification-MEP-ESNA.pdf)
- Develco oplyser at det er en prototype og kun kan købes hvis vi vil bestille 100.000 stk.
- Her opgav vi… Tak fordi i lyttede, nogle spørgsmål? ;-)

”Pludseligt lander et modul hos os” ☺

- Gammeldags reverse engineering af PCB for at finde MEP 6 pins header pinout
- Vi ”får fat” i CONFIDENTIAL PDF, med skrueterminalernes mening og at det er standard seriel/RS232
- Datadump med USB-serial adaptere og ”man in the middle” print (9600,n,8,1)
- Finder gammelt GitLab projekt der skulle være læsning af elforbrug på Echelon MEP port
- GitLab projekt er ”vildand” – det vi ser i vores datadump er slet ikke de samme…
  Enten forstår vi ikke GitLab projektet eller også har det aldrig virket?
  https://ressel.fh-salzburg.ac.at/FREDOSAR-Frapps/Smartmeter/smartmeter-fredosar-application/-/tree/master/org.fredosar.application.device.smartmeter.echelon
- Her opgav vi… Tak fordi i lyttede, nogle spørgsmål? ;-)

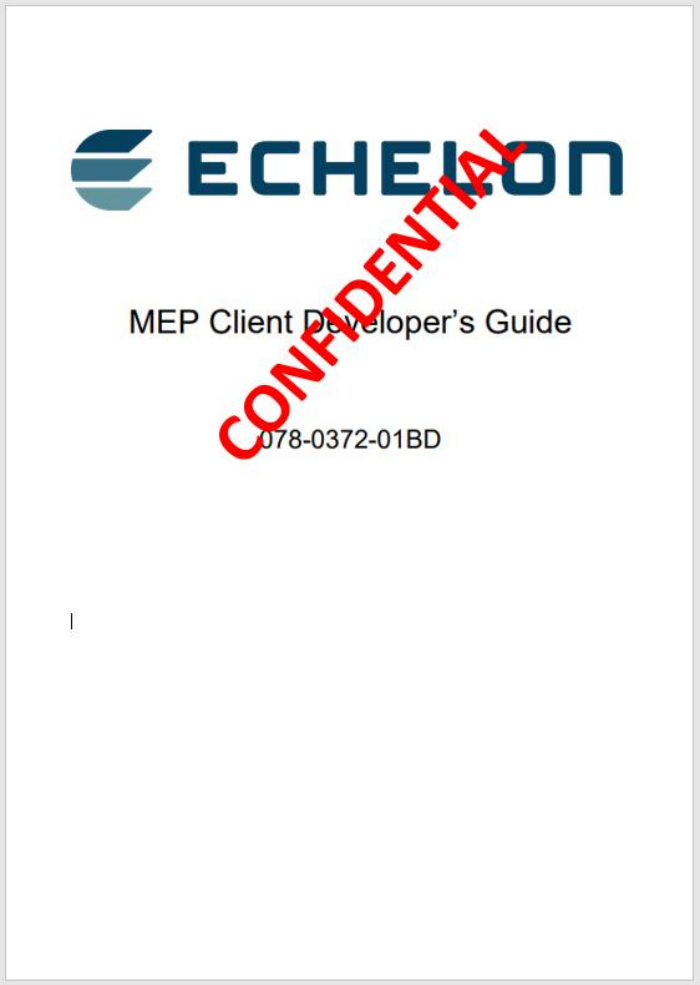
Electrical Specification

Meter Terminal	Name	MEP Direction	Function	RS232 DB9 Pin	RS232 DB25 Pin	Comments
14	M-Bus(+)	O	M-Bus Power			4kV isolated M-Bus port (+)* (+12Vdc/+24Vdc)
15	M-Bus(-)	I/O	M-Bus Data			4kV isolated M-Bus port (-)*
16	MEP_PWR	O	MEP POWER	NC	NC	+24Vdc nominal for 8XXX1-XXXX meters and 8XXX2-XXXX meters manufactured before 2013. +26Vdc for 8XXX2-XXXX meters manufactured in 2013 and after. *
16A	MEP_COM_TXD	O	MEP TXD	2	3	Meter's Transmit
17	MEP_COM_RXD	I	MEP RXD	3	2	Meter's Receive
18	MEP_COM_ENABLE	I	MEP COM ENABLE	7	4	MEP +12V/+5V Interface Enable
19	MEP_COM_GND	-	MEP GND	5	7	MEP GND Interface Power

```
00                                                  .
00 14 3f 00 34 00 00 00 00 08 00 00 00 01 13 7b  ..?.4..........{
3c 8b 5d 46 51 59                                <‹]FQY
00 14 3f 00 34 00 00 00 00 08 00 00 00 02 38 26  ..?.4.........8&
c6 2d 60 9d 91 83                                Æ-`‘ƒ
00 14 3f 00 34 00 00 00 00 08 00 00 00 03 7a 5c  ..?.4.........z\
0c de ea 0e 61 43                                .Þê.aC
00 14 3f 00 34 00 00 00 00 08 00 00 00 04 1c 9c  ..?.4..........œ
ad 6f 47 a5 ee ce                                -oG¥îÎ
00 14 3f 00 34 00 00 00 00 08 00 00 00 05 f5 e6  ..?.4.........õæ
7e 3e 50 07 a9 ee                                ~>P.©î
00 14 3f 00 34 00 00 00 00 08 0f 27 c6 4e 5a 9b  ..?.4......'ÆNZ›
6d ba 76 8e 79 0d 00 14 3f 00 35 00 00 00 00 06  mºvŽy...?.5.....
0f 27 c6 4f bf 25 5d 36 7d 4d 7e 8d 00 14 3f 00  .'ÆO¿%]6}M~..?.
37 00 00 00 00 08 0f 27 c6 50 c9 2b 35 ba da 07  7......'ÆPÉ+5ºÚ.
7f 17 00 14 3f 08 0b 00 00 00 00 18 0f 27 c6 51  ▯...?........'ÆQ
23 8f 54 bc a4 9d 6c 6c                          #T¼¤ll
00 14 3f 08 0e 00 00 96 00 02 0f 27 c6 52 ea 70  ..?....–...'ÆRêp
17 8d df 68 7b f0 00 14 3f 08 04 00 00 04 00 06  .ßh{ð..?.......
0f 27 c6 53 54 0b ee b7 9d 05 14 ac 00 14 3f 00  .'ÆST.î·..¬..?.
15 00 00 00 00 09 0f 27 c6 54 48 67 3c db f0 44  .......'ÆTHg<ÛðD
ae 63 00 14 3f 08 0e 00 00 05 00 01 0f 27 c6 55  ®c..?........'ÆU
4e e4 6a db 3a 9c e1 e5                          NäjÛ:œáå
```

Skjult port med hemmelig protokol

- I ren desperation skrev vi til NES' (Networked Energy Services) support. Og forventede intet svar/ingen hjælp
  https://www.networkedenergy.com/
- Vi fik et teams møde i stand med en Senior Vice President hos NES
- Timing var perfekt, NES ville gerne hjælpe
- Men MEP protokollen er hemmelig. Vi måtte underskrive Non-Disclosure Agreement (NDA) for at komme videre med projektet
- Ukrypteret MEP port?
  Jo-vist, men med digest (checksum), der skal bruge nøgle som vi skal have fra N1
- 3 niveauer af nøgler – nogle ting kan læses men den ene men kun skrives af den anden:
  - "No key required": …men ok at bruge en alligevel
  - MBK: MEP Basic key (aka BEK/Base Encryption Key)
  - MAK: MEP Advanced key (aka OMAK/Open Media Access Key)
- At få nøgler ud af N1!?!??!
  Her opgav vi… Tak fordi i lyttede, nogle spørgsmål? ;-)



N1 to the rescue

- Helt som forventet ville N1 overhovedet ikke høre tale om at udlevere MAK nøglen… Efter sigende kan den bruges til næsten alt på interfacet og er unik per måler
- Helt MOD vores forventninger ville N1 GERNE udlevere MBK nøglen, som umiddelbart kan læse alt hvad der er relevant for at følge forbruget – og mere…
- N1 vil ikke have vi giver jer nøglen. Kontakt jeres el-handler (der hvor i køber jeres strøm) – de kan så bede netleverandøren (dem der ejer jeres ledning og måler, i vores tilfælde N1) om at udlevere nøglen til jer. Det gør de via en webform.
  I skal blot spørge efter: ”Læse-nøglen til elektronisk aflæsning af Echelon-målere (I skulle kunne sende forespørgslen videre til N1 via en webform, så de kan sende nøglen til mig)”.
  Det er nok en fordel at medsende oplysninger om installationsnavn/adresse, måler-nr. og installations-nr.
- En MBK er på 16 eller 20 bytes, så hvad gør man når man får noget tilbage der ligner 10 hex encodede bytes? (fx ”53540BEEB79D0514AC00”). PS: Fiktiv nøgle ☺
- Spildte meget tid på at beregne med forkerte nøgler og på de første af de pakker som vi dumpede fra ZigBee / MEP printet – vi kunne IKKE beregne samme digest (checksum) og måleren ville ikke svare…
- Her opgav vi… Tak fordi i lyttede, nogle spørgsmål? ;-)

Hej Norlys,

Jeg har fået at vide kan jeg kan rekvirere en læse-nøgle til elektronisk aflæsning af min Echelon måler via jer.
(I skulle kunne sende forespørgslen videre til N1 via en webform, så de kan sende nøglen til mig).
Vil i sætte det i gang?

Mit målernr. er:
Mit installationsnr. er:

Med venlig hilsen

Navn
Email
Etc.

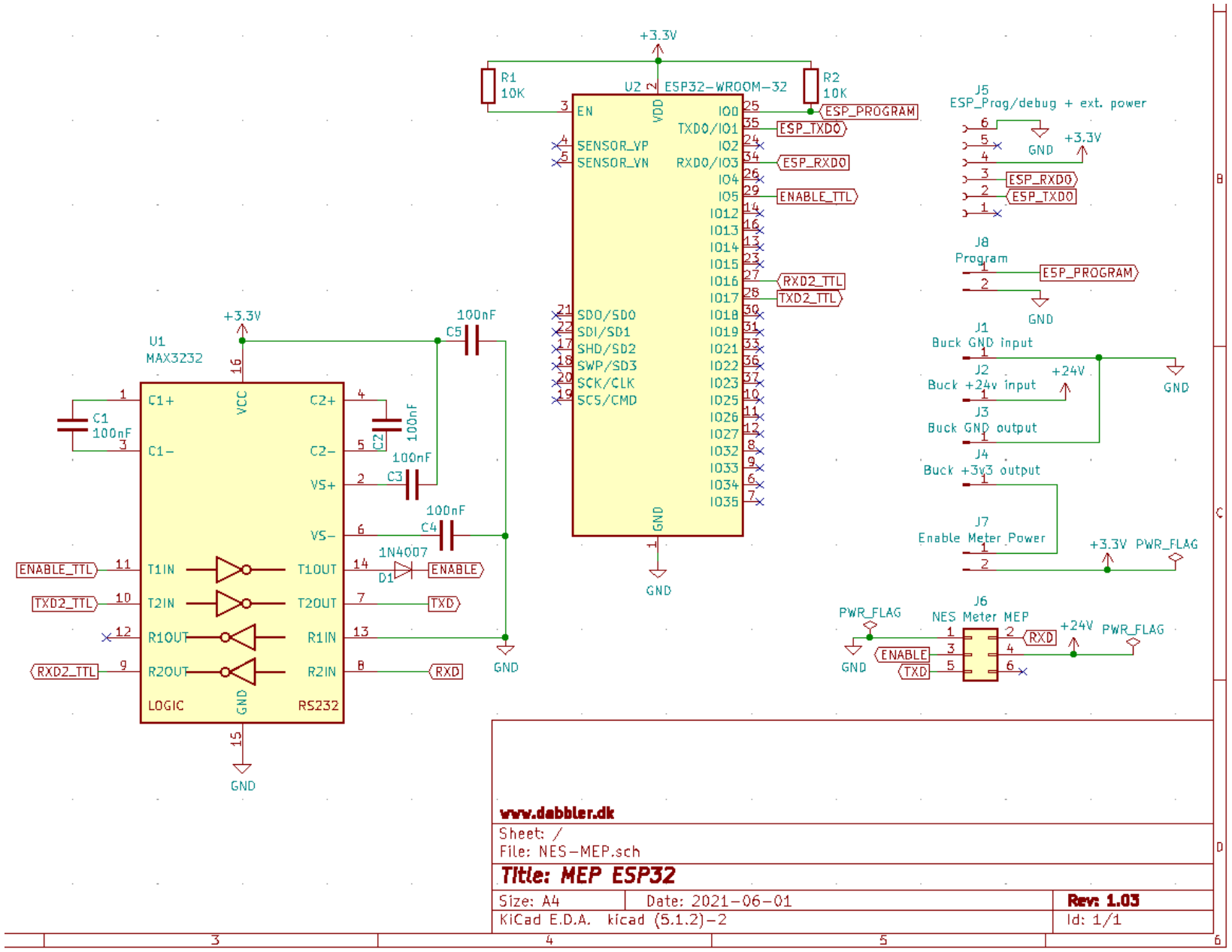
NES to the rescue

- Vi fik igen hjælp fra en teknisk kontakt hos NES:
  - Selv om det N1 udleverer ligner en 10 byte hex encoded string, så er det faktisk en ASCII string. Dvs. man skal tage ASCII værdien fra hver tegn og får dermed de krævede 20 bytes!
    PS: Hvem f**den hos N1 eller NES har besluttet at koden skulle ligne en hex string når de ikke er en hex string!?!?!?

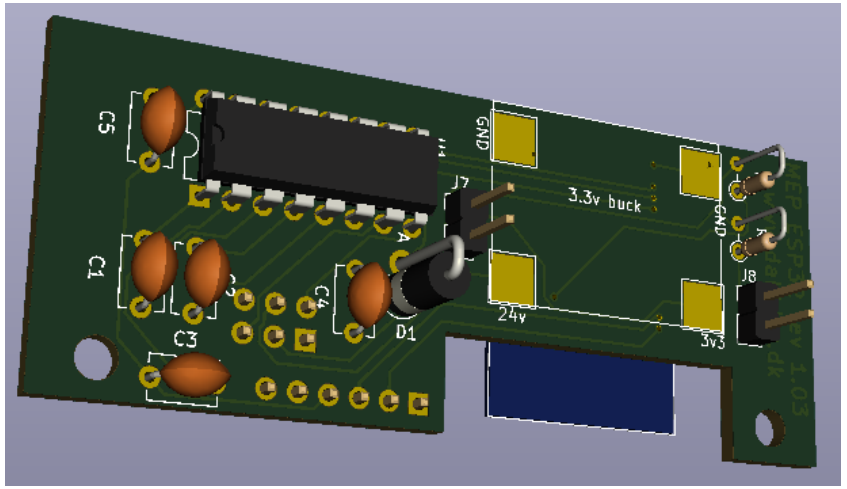
  - ZigBee / MEP modulet prøver med flere forskellige nøgler indtil den finder den rigtige (den har formentligt flere indbygget i softwaren), så eftersom vi kun kiggede på de første pakker der blev sendt fra modulet – så vi aldrig en digest, der blev beregnet med den MBK vi har!

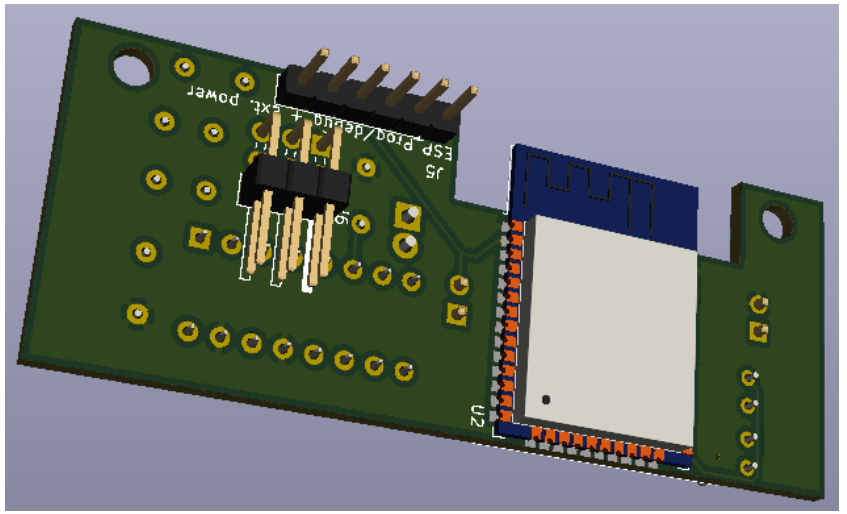
- Success! Vi har nu alle brikkerne til ”puslespillet” – nu skal de blot lægges!

Hardwaren – efter et par revisioner ☺

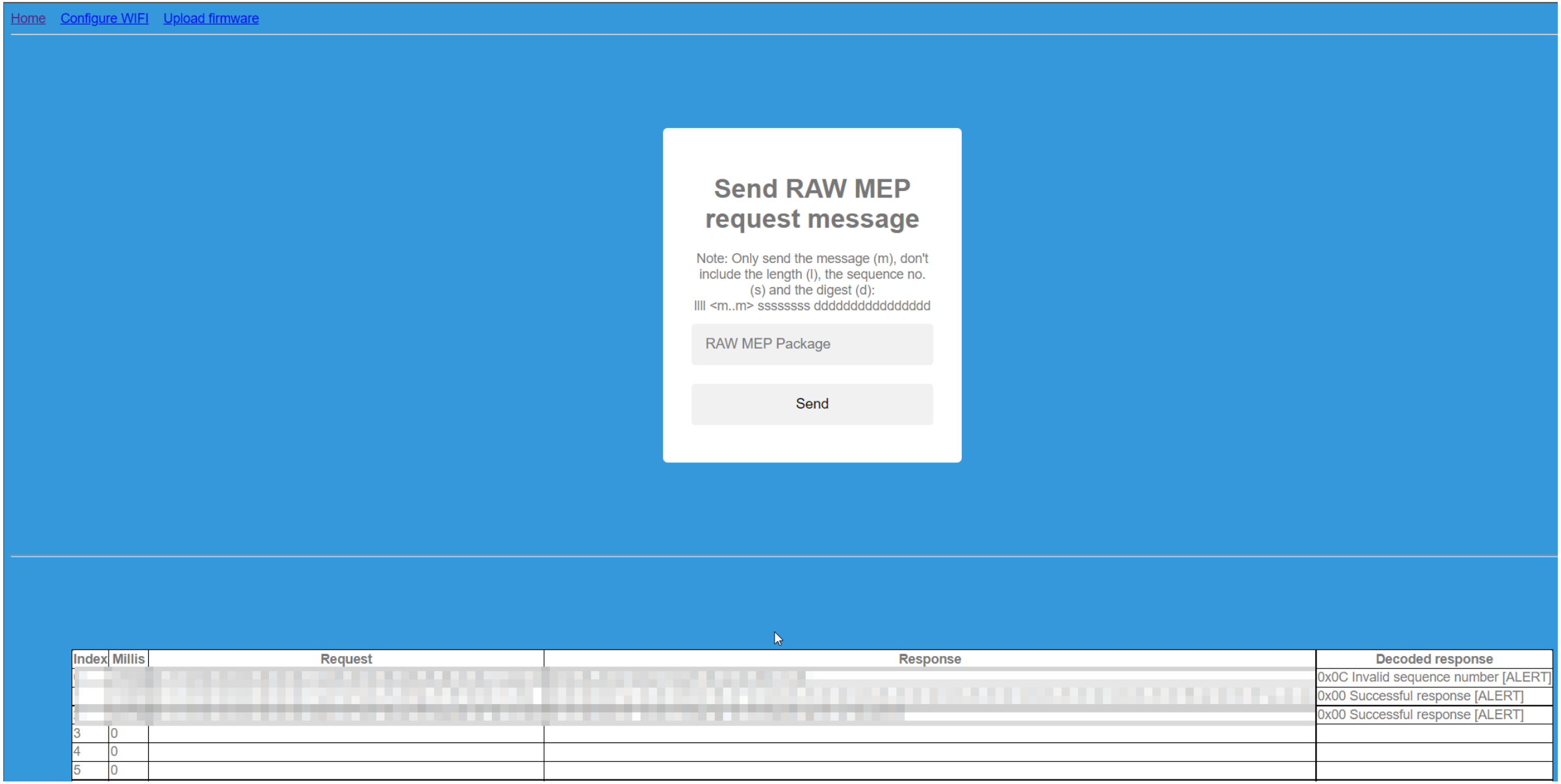


Begrænset plads: 60 (70) * 28 mm
Begrænset strømforbrug: max 1 watt





Softwaren – stadig lidt rå



Den hemmelige MEP protokol (1/3)

…sorry…

Den hemmelige MEP protokol (2/3)

Men lidt kan vi da fortælle:

- MEP protokollen er langt mere kompleks end man ville gætte
- I måleren findes der 80 tabeller og 30 procedurer
- Procedurer afvikles ved at skrive dem i en tabel og senere aflæse resultatet. De kan som option afvikles flere ad gangen i en transaktion
- Der er (begrænset) mulighed for at konfigurere og skrive i displayet, mulighed for at andre målere kan aflevere data, som så kan medsendes el-forbrugsdata når måleren automatisk aflæses
- Der er mulighed for at man fra central hold kan sende filer (fx ny firmware) til MEP modulet
- Rigtigt mange aspekter af el-leverancen kan aflæses: forbrug (til dato og løbende), frekvens, faseforskydning osv.
- MEP-moduler kan registrere sig på målerne (der vises et M i displayet), men det er ikke nødvendigt hvis man kun læser fra måleren. Modulet kan de-registrere sig igen
- Flere aspekter omkring M-Bussen kan kontrolleres fra MEP

Disclaimer:

TBD: Vi ved endnu ikke hvilke dele af protokollen, der bliver frigivet – og visse af ovenstående funktioner kræver MAK-nøglen (som N1 ikke vil udlevere). Så flere af disse funktioner bliver IKKE muligt med den adgang vi får.

Den hemmelige MEP protokol (3/3)

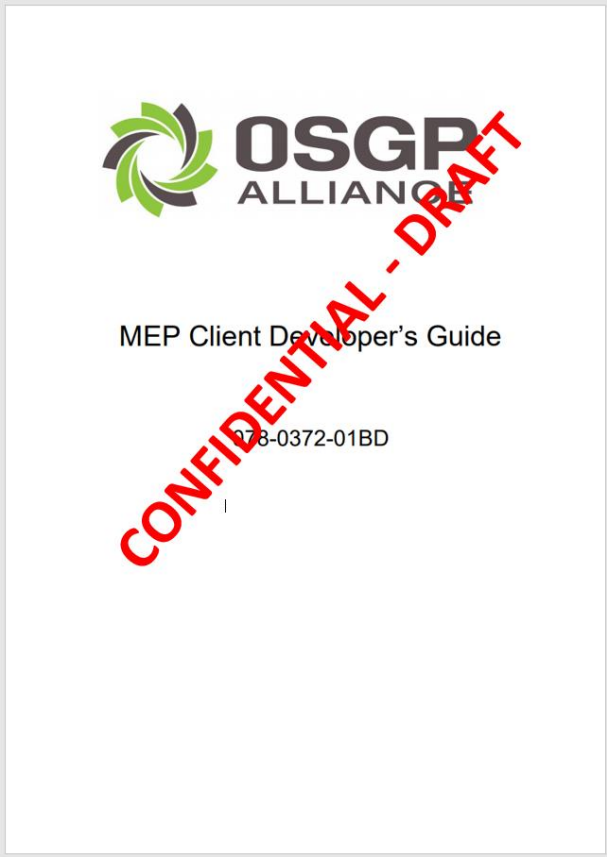
- Datapakker der sendes og modtages er binære bytes (dvs. ikke umiddelbart læsbart)
- Felter i datapakker kan være forskellige datatyper, fx bit, byte, word, long, ASCII strings etc.
- De pakker der sendes til måleren består af:
  - Datapakken (ved skrivning)
  - Fortløbende sekvensnr. på pakken
  - Læse/skrive kommando, med parametre (fx position og længde af data der læses/skrives)
  - Digest (en form for checksum, der beregnes ud fra pakkens indhold og den anvendte MAK-/MBK-nøgle)
  - Pakkens længde

- De pakker der modtages fra måleren består af:
  - Digest (en form for checksum, der beregnes ud fra pakkens indhold og den anvendte MAK-/MBK-nøgle)
  - Pakkens længde
  - Status-byte
  - Datapakken

- Måleren kan sende et alarm-flag til MEP modulet, og MEP modulet SKAL håndtere dette ved at aflæse fejllog mv. Ellers black-listes modulet…

Er det Juleaften nu?

- ”Vores” Senior Vice President hos NES er også bestyrelsesmedlem i OSGP Alliance og derudover vist også selv lidt af en ”tinkere”…
- …han var i øvrigt med i det Echelon-team, der solgte de fleste (alle?) Echelon målerne til elselskaberne i Danmark…
- …og har besluttet at read-only delene af MEP- og IR-protokollen skal frigives som en form for ”open source” i OSGP Alliance regi
  https://osgp.org/
- IR-protokollen ER frigivet som OSGP Alliance dokument
- Ting tager tid, men vores kontakter hos NES og OSGP Alliance arbejder i øjeblikket på at omforme ”MEP Client Developers Guide” til et OSGP Alliance dokument, der kun indeholder de ting der skal bruges for at kunne læse fra måleren.
- Så ”om lidt” kan du selv lave hardware og software til MEP. Release date? Q4 2021 – hold øje med https://osgp.org og https://www.dabbler.dk



What's next?

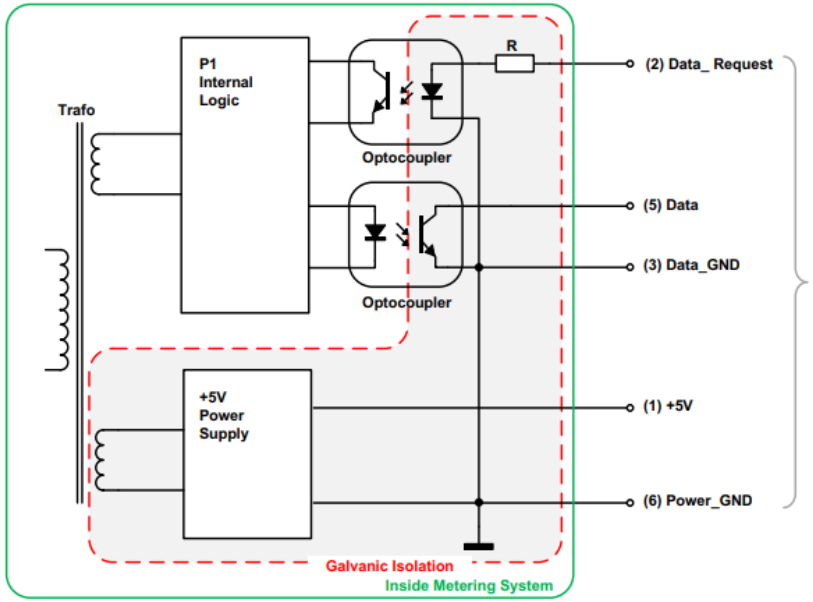
INTET er fastlagt – tiden og fantasien sætter grænserne!

- Indlæg om forløb på www.dabbler.dk
  (er klart, men vi ville først holde dette indlæg)

- Indlæg om protokol-detaljerne på www.dabbler.dk
  (når vi er fri af vores NDA med NES / når de har frigivet protokolbeskrivelserne)

- Dele hard- og software på GitHub og få flere involveret?

- Hard- og Software idéer:
  - Beskyt med login+password så "siderne" kan deles på nettet
  - Konfiguration udbygges med MBK, login+password etc.
  - Tinkering side forbedres
  - Ny side med dashboard med løbende opdatering (grafisk præsentation?)
  - MQTT med løbende målinger og low level protokol
  - Webservice med løbende målinger og low level protokol
  - "Ny" RJ12 standard (kaldet P1 i Holland og H1 i Sverige)
  - Integration mod div home automation systemer



Spørgsmål? + kontaktinformation

Graves Kilsgaard
https://www.linkedin.com/in/kilsgaard/
graves@dabbler.dk

Gert Lynge
https://www.linkedin.com/in/gertlynge/
gert@dabbler.dk