

# Security analysis of Dutch smart metering systems

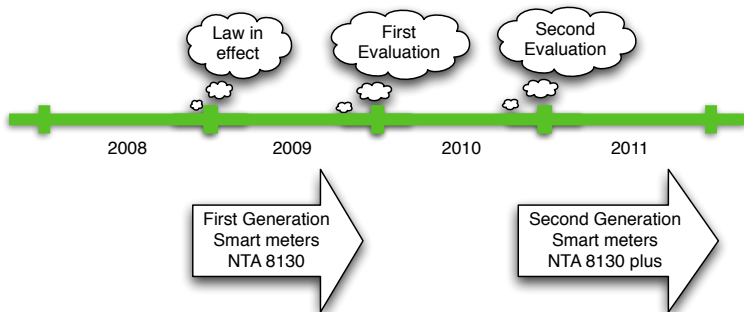
Sander Keemink and Bart Roos

July 2, 2008

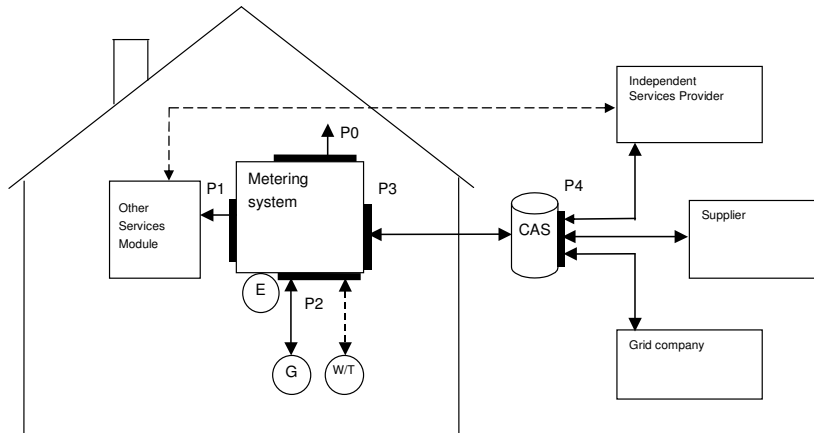
- 1 Smart metering introduction
- 2 Theoretical research
- 3 Practical research
- 4 Recommendations
- 5 Conclusion

# Smart Metering goals

- Accurate billing
- Insight in energy usage
- NTA Dutch Technical Agreement

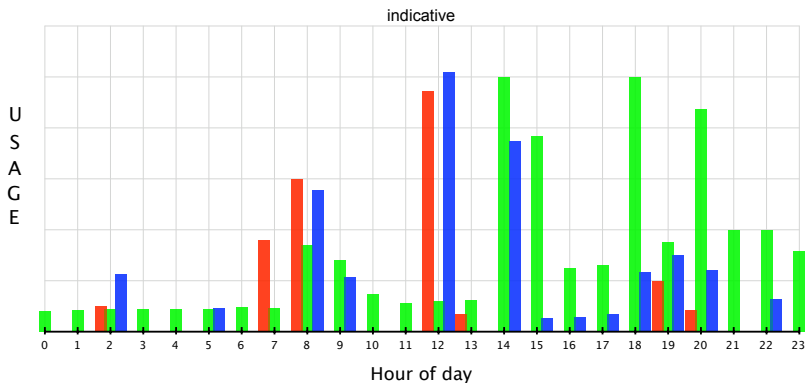


## NTA



# Your energy usage

- What do you see in this image?



Electricity Water Gas

## Research objective

*“Analyze the possible impact of the use of smart metering systems on the security of electricity metering using the CIA-triad and minimum requirements as stated in the NTA-8130 regulation. Compare the NTA and a preferred situation with the smart metering systems that are currently implemented.”*

# Theoretical research

- Defined the need for security using the CIA-triad
- Analyzed the NTA security requirements:

P0	Not defined
P1	Read-only
P2	Encryption allowed if interoperable
P3	Grid operator should take 'appropriate measures'
P4	Grid operator should take 'appropriate measures'
P5	Out of scope

- Defined possible attack vectors based on CIA-triad

# Port 0 security

- Optical interface (all meters)
- Programming buttons (some meters)
- Security measures
  - Switch behind security seal
  - Tamper detection





# Port 0 security

MAP120 - [IEC Service Tree : LGZZMF100AC\_M12 \*]

File View Communication Extras Window Help

Landis+Gyr MAP120 DLMS METER TOOL [Demo Version]

65000 : : LGZZMF100AC\_M12

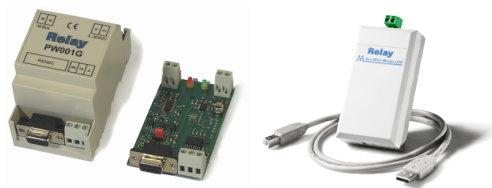
- [-] 60112 : IEC1107+ Readout
  - 60212 : Readout = [=F.F(00)]=C.1.0(88903893)]=0.0(KA2Q008890389307)]=C.
- [+] 60102 : IEC1107+ Time and Date
- [+] 60103 : IEC1107+ Meter Identification
- [+] 60104 : IEC1107+ Billing Period Reset
- [+] 60105 : IEC1107+ Diagnostics
- [+] 60104 : IEC1107+ Communication
- [+] 60106 : IEC1107+ Passwords
- [+] 60107 : IEC1107+ Test Mode
- [+] 60108 : IEC1107+ Reset Registers and Stored Values
- [+] 60109 : IEC1107+ Load Profile
- [+] 60110 : IEC1107+ Event Log
- [+] 60115 : IEC1107+ Enable / Disable Energy Registers on Display

60212 : Readout

```
F.F(00)
C.1.0(88903893)
0.0(KA2Q008890389307)
C.1.1(94888007)
1.8.1(0001300.3*kWh)
1.8.2(0001166.8*kWh)
1.8.0(0002467.2*kWh)
2.8.0(0000000.0*kWh)
15.8.0(0002467.2*kWh)
C.7.0(0006)
32.7(227^V)
52.7(001^V)
72.7(000^V)
C.5.0(38)
```

## Port 2 security

- Wired
  - M-Bus without encryption
  - M-Bus interfaces widely available
  - Simulate gas or water meter (slave)
  - Simulate electricity meter (master)



- Wireless
  - Proprietary protocols
  - Wireless M-Bus not being used

## Port 3 security

- Communication methods:
  - PowerLine Communication (PLC)
  - GPRS
  - Ethernet
  - Radio Frequency mesh (RF)
- Risks
  - Sniffing (Serial GPRS modem and Ethernet)
  - Disrupting communications
  - Denial of Service attacks

# Port 3 security

WebRTU z1

http:// / Inquisitor

Apple Yahoo! Google Maps YouTube Wikipedia Nieuws (971) Populair Serialtest Se...cket Sniffer

**ENERGY IT** Providing Tomorrow's Energy Management Solutions, Today. **WEB RTU z1**

Energy Information and Communication Technologies

**Reports**

- [Today](#)
- [Yesterday](#)
- [This Week](#)
- [Previous Week](#)
- [This Month](#)
- [Previous Month](#)
- [All Values](#)
- [MRs - Indexes](#)
- [Status](#)
- Configuration**
- [Network](#)
- [RTU Parameters](#)
- [Time Server](#)
- [Modem](#)
- [PPP](#)
- [Channel Functions](#)
- [Channel Parameters](#)
- [Channel Name/Unit](#)
- [Meter Readings](#)

Date	Time	Code	Status	1	Gas (l)	Cold Water (l)	Heat (MJ)
2008/06/20	15:15:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	15:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:45:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:30:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	14:15:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	14:00:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	13:45:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	13:30:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	13:15:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	13:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	12:45:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	12:30:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	12:15:00	00	0000	0000000005	0001299080	0000007851	0000032896
2008/06/20	12:00:00	00	0000	0000000006	0001299080	0000007851	0000032896
2008/06/20	11:45:00	00	0000	0000000005	0001299080	0000007851	0000032896

# Port 5 security

- Risks
  - Sniffing
  - Man-in-the-Middle attack
  - Shoulder surfing for credentials
  - The usual risks
- Basic security measures
  - SSL (HTTPS)
  - Strong authentication



Welkom bij Mijn Oxxio!


Meer informatie op [Oxxio.nl](http://Oxxio.nl)

- [Contact & Vragen](#)
- [Meest gestelde vragen](#)
- [Download handleiding Mijn Oxxio](#)

### Welkom bij Mijn Oxxio

Volg en controleer uw energieverbruik via Mijn Oxxio. Deze persoonlijke en beveiligde pagina hoort bij uw slimme meter. U kunt bijvoorbeeld uw verbruik per week, per maand of zelfs per jaar bekijken. Zo weet u precies wat uw verbruik was over de verschillende periodes.

### Inloggen

Klantnummer:  

Postcode:

Huisnummer:  zonder toevoeging

Inloggen 

Mijn aansluitingen

Voortgang installatie

Verbruiksgegevens



Bekijk hier uw  
verbruiksgegevens!

## Verbruiksgegevens stroom

## Kies periode

Periode: Maand

Jaar: 2008

Maand: juni



## Mijn verbruik

Piek: 98.47 kWh

Dat: 92.05 kWh

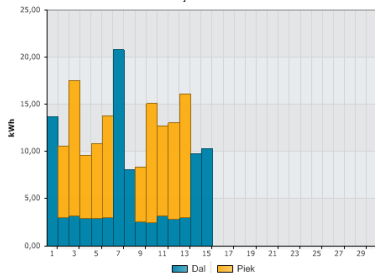
Totaal verbruik: 190.52 kWh

Percentage piek: 51,68%

## Mijn meterstanden

Piek

Geen gegevens

Energieprofiel  
juni 2008

Voor meer details klik op de betreffende dag in de grafiek

**oxxio**  
Slim met energie

U bent ingelogd als:

DemoKlant  
Storkstraat 17c  
3833 LB LEUSDEN  
Klantnummer: 9999998

Uitloggen

Meer informatie op [Oxxio.nl](http://Oxxio.nl)

- [Contact & Vragen](#)
- [Meest gestelde vragen](#)
- [Download handleiding Mijn Oxxio](#)

# Recommendations

## NTA:

- Aggregate data per day, week or month
- More specific security requirements in NTA
- Port 0 should be part of NTA
  - Including minimal security requirements



# Recommendations

Supplier and grid operators:

- Do not trust security seals
- Data availability can not be guaranteed
- Use open encryption on all links
- Do not underestimate privacy aspects
- Use SSL and strong passwords on website
- Perform data checks to verify correctness of data

# Conclusion

- Privacy underestimated
- NTA not specific enough about security
- Security of meter management functions not sufficient
- No secure channel between electricity and gas or water meter
- Supplier websites should improve their security

# Thanks

Thanks for your attention  
Any questions before enjoying your lunches?