The process to securing smart meters

2009-10-28

Gitte Bergknut, E.ON Sverige AB

Overview

- Historical background
- General rekommendations before the projects
- The Security interference
  - Understand the functional design and requirements
  - Risk analysis
  - Setting security demands
  - Experiences from intervjuing vendors
- What now?
- The strategical security circle

Historical background

- In 2003 the Swedish Goverment decide that exact monthly meter value reading is mandatory as the first country in the world.

- The law was controversial and both positive and negative arguments where discussed in public.

- High Cost presure

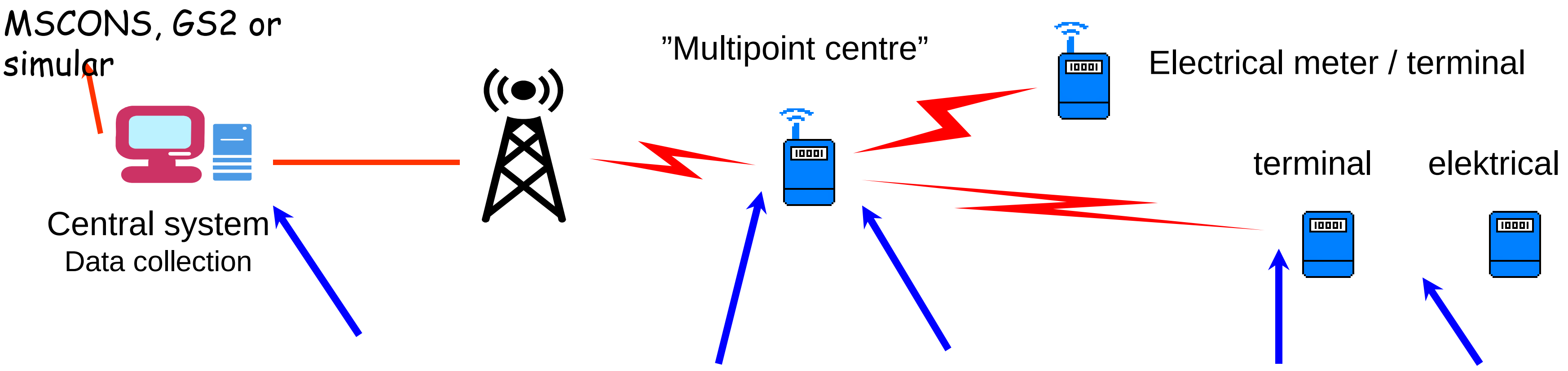
- The decision required a change of all meters to smart meters(5 million)

- The cost was estimated to between 5 to 10 billion SEK

- New technology and high number of meter 6 years = Short time frame

General recommendations to the Industry in 2003

- Over all design
- Specific requirement on customer display
- How often values should be collected
- Standard Communication protocol (TCP/IP)
- Standard component benefiting from over all IT technology development
- Expected life 18 years



Applikation level	Functional demand acc. Sv. Energi							Functional demand acc. Sv. Energi
Protokolls level	TCP/IP		TCP/IP		TCP/IP		TCP/IP	S0, 1107, Mbus Or other open standard
Hardware level							PCMCIA USB, Modular	"Standard"

TCP/IP: Is hardly suitable until TCP/IP version 6 is implemented.

Translated from a Svensk Energi presentation with recommendations 2003

General recommendations to the Industry in 2003

Open issues to investigate

- Changes in legal requirements such as
  - change of measuring date
  - collection and reporting of values
- Availability
  - Communication security
  - Information protection
  - Failures
- Physical interface
- Simple installation with fast connection of meter

Top focus back in 2003

1. Functional requirement

2. Project time and vendor deliverability

3. Cost

…

XX. Securing that meter value can be collected

This was the trigger to involve Security staff in the project = Me

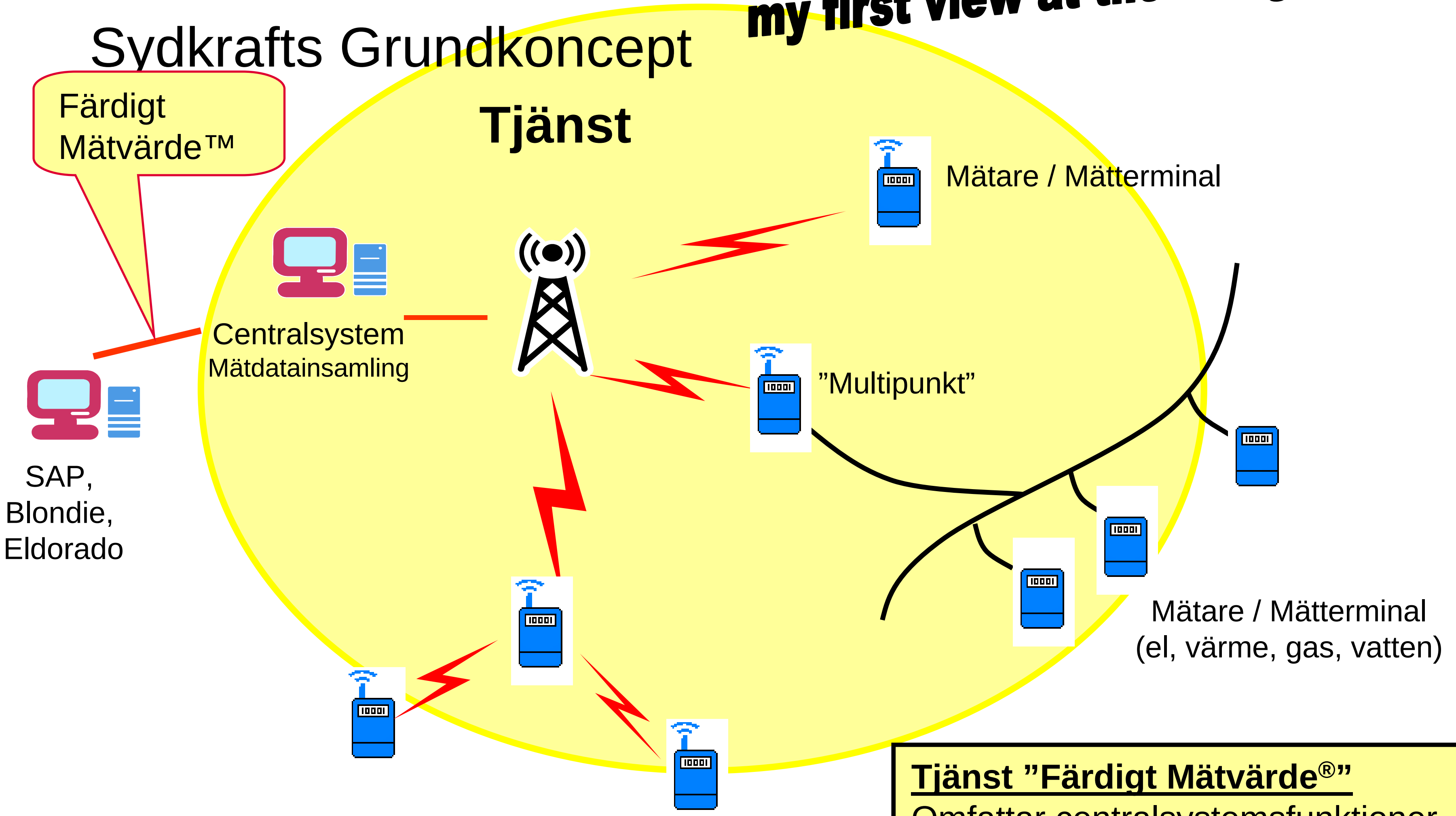
The Security interference!

- Mission nb 1:
  Understanding the functional design and requirement

- How: I went to visit our grid company and they showed me a picture….

my first view at the design in 2004

Sydkrafts Grundkoncept



Färdigt Mätvärde™

Tjänst

Centralsystem
Mätdatainsamling

SAP,
Blondie,
Eldorado

Mätare / Mätterminal

”Multipunkt”

Mätare / Mätterminal
(el, värme, gas, vatten)

Tjänst ”Färdigt Mätvärde®”
Omfattar centralsystemsfunktioner,
Kommunikation samt
drift/felavhjälpning
av hela systemkonceptet

My reaction

- OOOhhh ….
- Then lots of

Have You done a risk analysis ?

Is this wireless?

???????

What are the protocols?

No!

FTP???

<u>What is the data?...and how is it classified?</u>

Technical requirements?

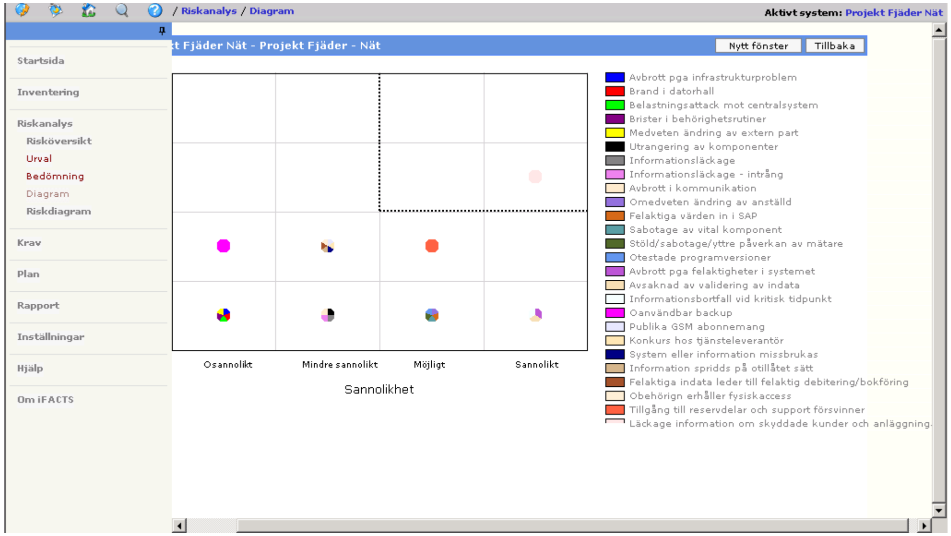
TCP/IP???

Modem?

Access control???

Risk analysis

- Scenario based qualitative risk analysis where conducted in December 2004.
- With our corporate information security management tool (LISA).
- Most scenarios wasn't judged as serious, except one, at the time.
- The most serious scenario was data leakage of data regarding customers.
- System unavailability at critical time and lack of spare parts where assumed to be high risk.



/ Riskanalys / Diagram
Aktivt system: Projekt Fjäder Nät
Startsida
Inventering
Riskanalys
Risköversikt
Urval
Bedömning
Diagram
Riskdiagram
Krav
Plan
Rapport
Inställningar
Hjälp
Om iFACTS
t Fjäder Nät - Projekt Fjäder - Nät
Nytt fönster
Tillbaka
Osannolikt
Mindre sannolikt
Möjligt
Sannolikt
Sannolikhet
Avbrott pga infrastrukturproblem
Brand i datorhall
Belastningsattack mot centralsystem
Brister i behörighetsrutiner
Medveten ändring av extern part
Utrangering av komponenter
Informationsläckage
Informationsläckage - intrång
Avbrott i kommunikation
Omedveten ändring av anställd
Felaktiga värden in i SAP
Sabotage av vital komponent
Stöld/sabotage/yttre påverkan av mätare
Otestade programversioner
Avbrott pga felaktigheter i systemet
Avsaknad av validering av indata
Informationsbortfall vid kritisk tidpunkt
Oanvändbar backup
Publika GSM abonnemang
Konkurs hos tjänsteleverantör
System eller information missbrukas
Information spridds på otillåtet sätt
Felaktiga indata leder till felaktig debitering/bokföring
Obehörign erhåller fysiskaccess
Tillgång till reservdelar och support försvinner
Läckage information om skyddade kunder och anläggning

Setting Security requirement

- The first issue was to get a confidentiality agreement before handing out the purchasing material with all potential partners.
  - Why was this important? Well to get a proper business calculation in the offer the partners needed to know how many and where we had customers. Data that we regard as confidential, in some cases really sensitive to the customer or third part, and it had to be a official open procurement according to Swedish law.

- Then we created Amendment 18 Security demands in the project requirement specification based on.
  - The risks found in the risk analysis
  - General corporate security requirements at the time
  - ISO 17799

Selecting partners and vendors

- The project received approximately 20 different offers
- Most of them had more or less..
  - No technical security mechanism except backup for central system
  - No information security policy and routines

- In the interview I understood that the vendors had very little knowledge of IT security

- Internally – The security considerations where more about physical parameters

- But the 10 interview where I participated had lots of interesting discussions and became a awareness travel for all involved including me

But with the eyes and knowledge of today

Proberly this would be ranked must higher

- Public GSM.
  Consequence less serious and less probably.
  Somebody with technical knowledge calls the GSM number and crack the FTP login at the meter then establishes a connection from meter to concentrator and insert malware. The malware give control and manipulation possibility of the communication through the concentrator or access point to central system. Possible outfall: mass manipulation of data and data leakage regarding customer.

Requirements:
Secret and closed number group for meters and concentrators,
no password login to end component and checksum to all transmitteds value
Encryption was disregarded due to cost and technical difficulties.

Why was the scenarios judged so low?

- Lack of knowledge and understanding
  - The control people didn't se the IT threats and as a IT security specialist with mostly experiences with administrative system I didn't see the full consequence.
  - The condition was the meters can only read the consumption by the customer not disconnect electricity.

- But today in Sweden and in many other countries can the meters
  - not only be used for remote reading of consumption
  - they can also be used for remotely connect and disconnect power.

So is the risk low today?

Security experts have this summer demonstrated worms that can use weaknesses in most meters from several different vendors.

We still don't have TCI/IP v6 but we do use TCP/IP according to recommendation.

Remote control of electricity is regarded both as a business opportunity to lower cost and a customer requirement.

Consequence: Severe

Probability: High

Status today

- The Industry cost is not known, but estimated to 15 billion SEK but the reform is regarded as positive and successful.
- In the beginning of June 2009 the role-out project at E.ON closed after changing 1 000 000 meters.
- In the end all security requirements are stil not meet but the awareness has rosen.
- The president from one of the partners called me and said ”Thank you! Can you recommend me a information security consultant in the Stockholm are” another partner has started several internal security projects to increase the IT security of their products.
- E.ON is currently pilot testing remote control of meters in 3 different cities.