Smart metering: Cesta od mechanického elektroměru k chytrým sítím.

Ing. Radomír Kozub

14. prosince 2012

Tato prezentace je spolufinancována Evropským sociálním fondem a státním rozpočtem České republiky.

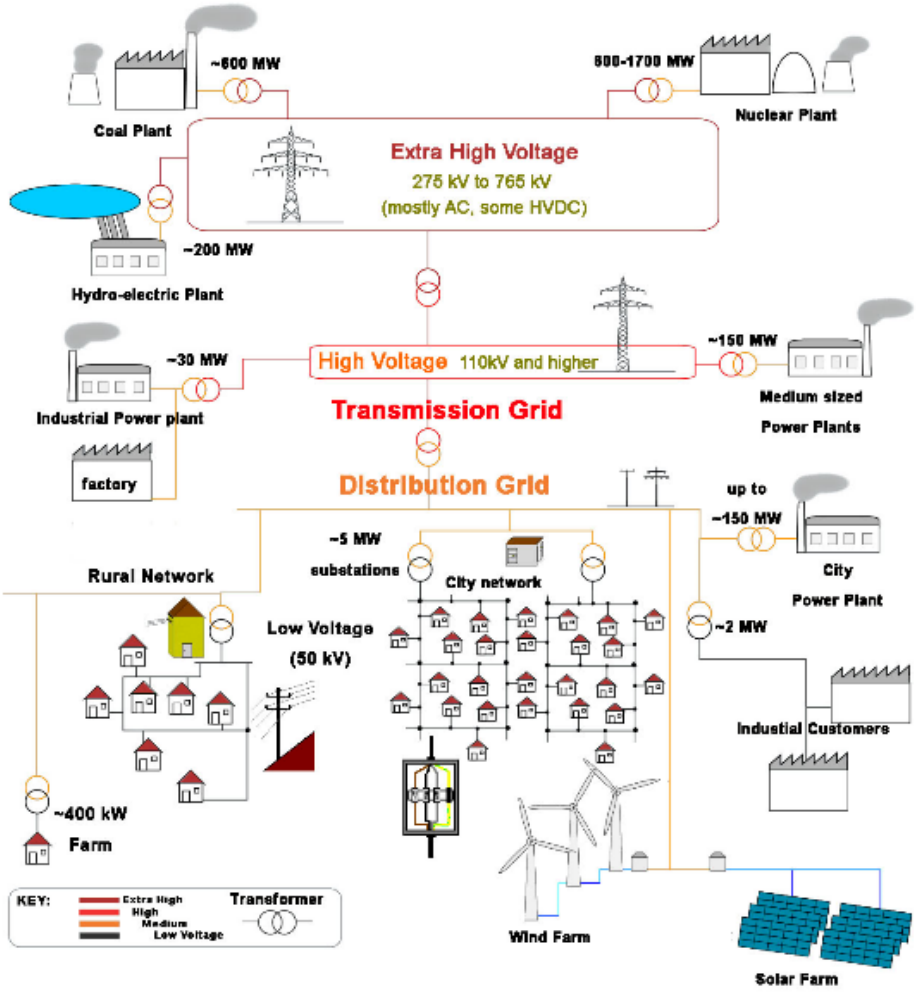
Agenda

- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- current, voltage sensors used in static meters
- single, two and three phase topologies
- energy calculation algorithms active and reactive energy
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- existing MCU overview

Agenda

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- security short review

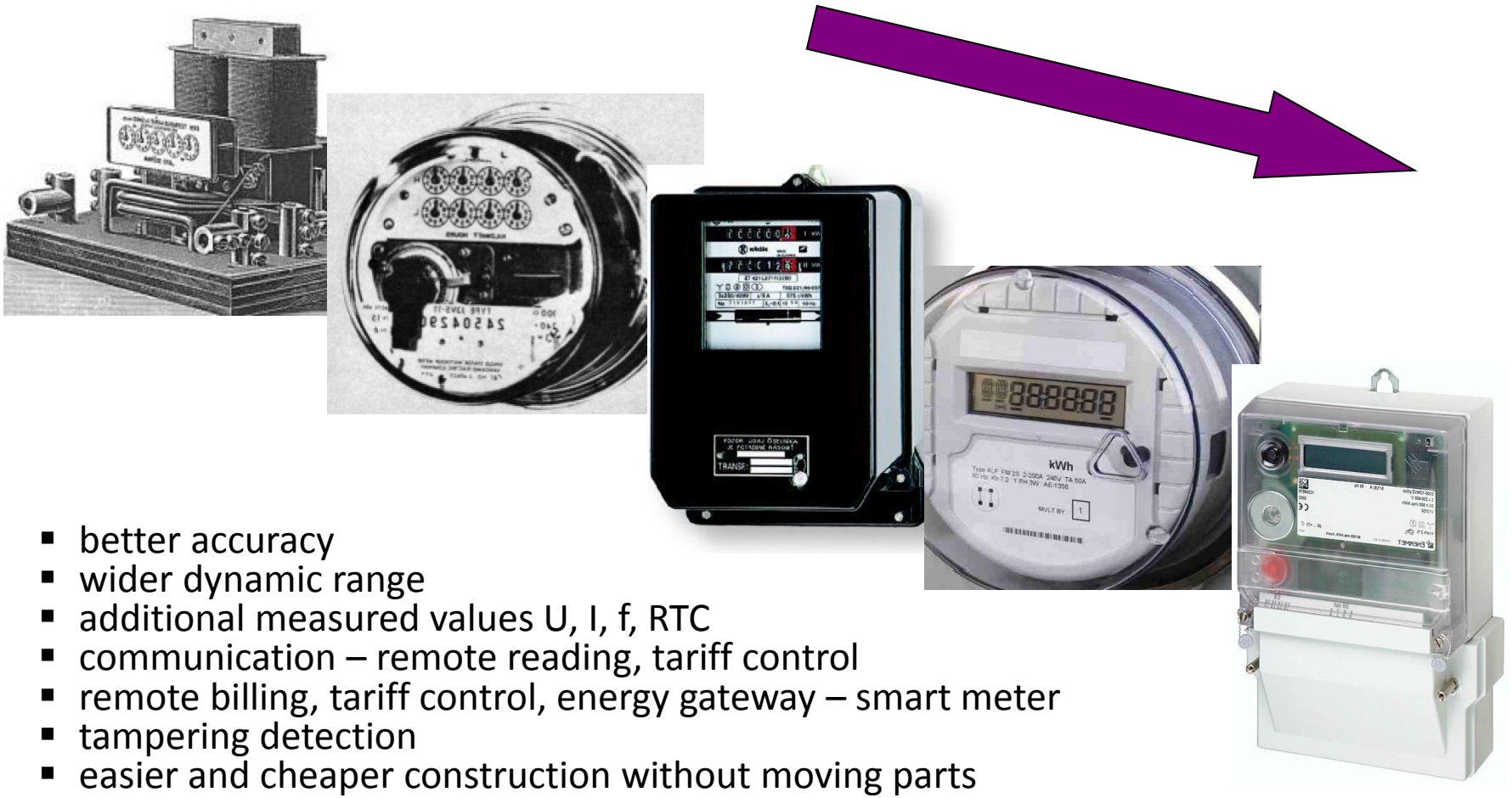
Smart Grid - what is it?



Accuracy requirements to actual power meters

- Smart Grid - general overview
- Power Meters
- **accuracy requirements to actual power meters**
- current, voltage sensors used in static meters
- single, two and three phase topologies
- energy calculation algorithms active and reactive energy
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- existing MCU overview

Electromechanical Power meters are replaced by static ones



- better accuracy
- wider dynamic range
- additional measured values U, I, f, RTC
- communication – remote reading, tariff control
- remote billing, tariff control, energy gateway – smart meter
- tampering detection
- easier and cheaper construction without moving parts

Basic requirement for static power meters required by EN 50470-3

Electricity Meter Types

Electromechanical meters

- *Limited accuracy*
- *Manual reading*
- *Contains moving parts (aluminum ring)*

Electronic meters

- *MCUs, DSPs and ASICs based*
- *Accurate measurement*
- *Enhanced security*
- *Equipped with AMR*
- *No moving parts*

Measured Quantities

- *Active, Reactive, Apparent Energy*
- *Active, Reactive, Apparent Power*
- *RMS, Peak Values (voltage/current)*
- *Line frequency*
- *Power Factor*
- *Temperature*

Measurement Types

Single phase

- *Common in EU residential meters*
- *One voltage and one current measurement*
- *Use of shunt resistors prevail due to system low-cost*

Dual phase

- *Common in US residential meters*
- *Two voltage and two current measurement*
- *Use of current transformers and Rogowski coils prevail*

Three phase

- *Used in industrial and commercial meters*
- *Three voltage and three current measurement*
- *Use of current transformers and Rogowski coils prevail*

Basic requirement for static power meters required by EN 50470-3

- standardized values
  - voltage 120-230-277-400-480 (V)
  - nominal current 5-10-15-20-30-40-50 (A)
  - maximal current - multiplies of nominal current
  - active power **P [W]**, reactive power **Q [VAR]** and apparent power **S [VA]** should be measured
- dynamic range @ accuracy
  - 230V, 5(60)A; 230V, 5(100)A, Class A(2), B(1), C(0.5)
- factors impacting accuracy
  - mains frequency
  - load power factor
  - harmonics in voltage and current
  - temperature
  - DC current
  - limited power consumption in current circuit

Basic requirement for static power meters required by ANSI C12.20

- Meters are typically quoted as Class **p**%: **r**(**m**)
  - where **r** is the reference current
  - **m** is the maximum current
  - **p** is the accuracy class 0.5%, 0.2% – i.e. Class 0.2: 30(200)A
- Standardized values
  - voltage 120-240-277-480 (V)
  - Frequency rating 60Hz
  - Current classes (reference amperes) 2(0.25)-10(2.5)-20(2.5)-100(15)-200(30)-320(50) (A)
  - Starting currents @ current classes 0.001, 0.01, 0.01, 0.05, 0.1, 0.16 (A)
  - active power P [W], reactive power Q [VAR] and apparent power S [VA] should be measured

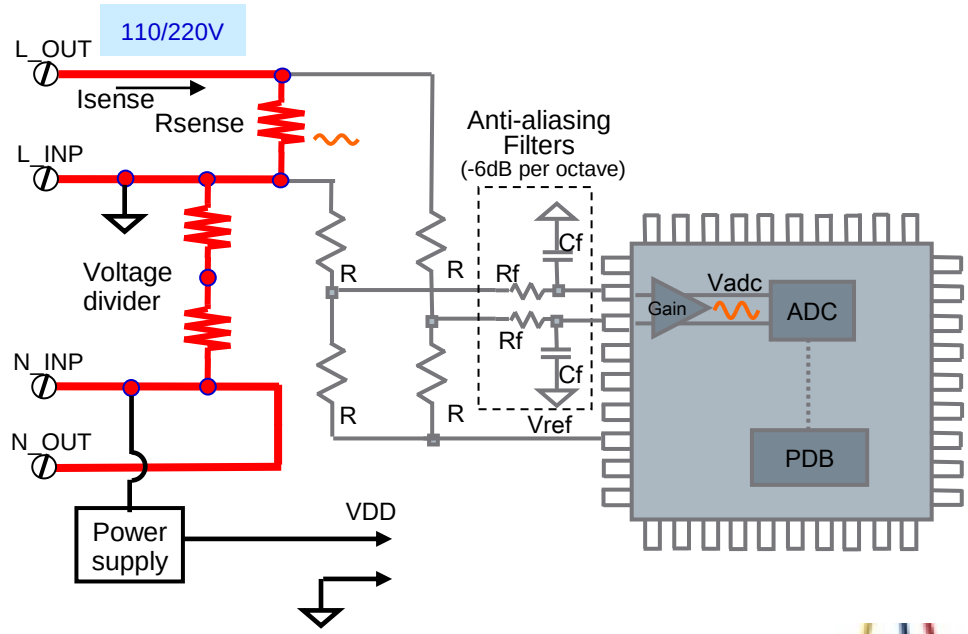
Basic requirement for static power meters required by ANSI C12.20

- Factors impacting accuracy
  - mains frequency
  - load power factor
  - harmonics in voltage and current
  - temperature
  - DC current
  - limited power consumption in current circuit

Current, voltage sensors used in static meters

- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- **current, voltage sensors used in static meters**
- single, two and three phase topologies
- energy calculation algorithms active and reactive energy
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- existing MCU overview

Current sensors - shunt resistor



Pros:

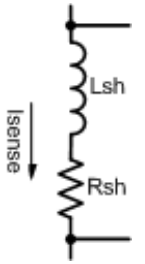
- *Commonly used*
- *Simple to design*
- *Inexpensive*
- *No magnetic effects*

Cons:

- *Self-heating due to power dissipation*
- *Parasitic inductance introduces phase shift at low power factors.*
- *Non-isolated*

Mathematical description:

$$I_{SENSE} = \frac{Vadc - \frac{Vref}{2}}{Gain * R_{SENSE}}$$



by courtesy of Zhongshan Weiqi Electronic

I_{SENSE}(A)	R_{SENSE}(Ω)	U_{SENSE}(V)
0.02	250μΩ / 170μΩ	5uV / 3.4μV
0.15		37.5uV / 25.5μV
60*		15mV / 10.2mV

* Power losses at 60A: 0.9W@ 250μΩ; 0.6W@170 μΩ

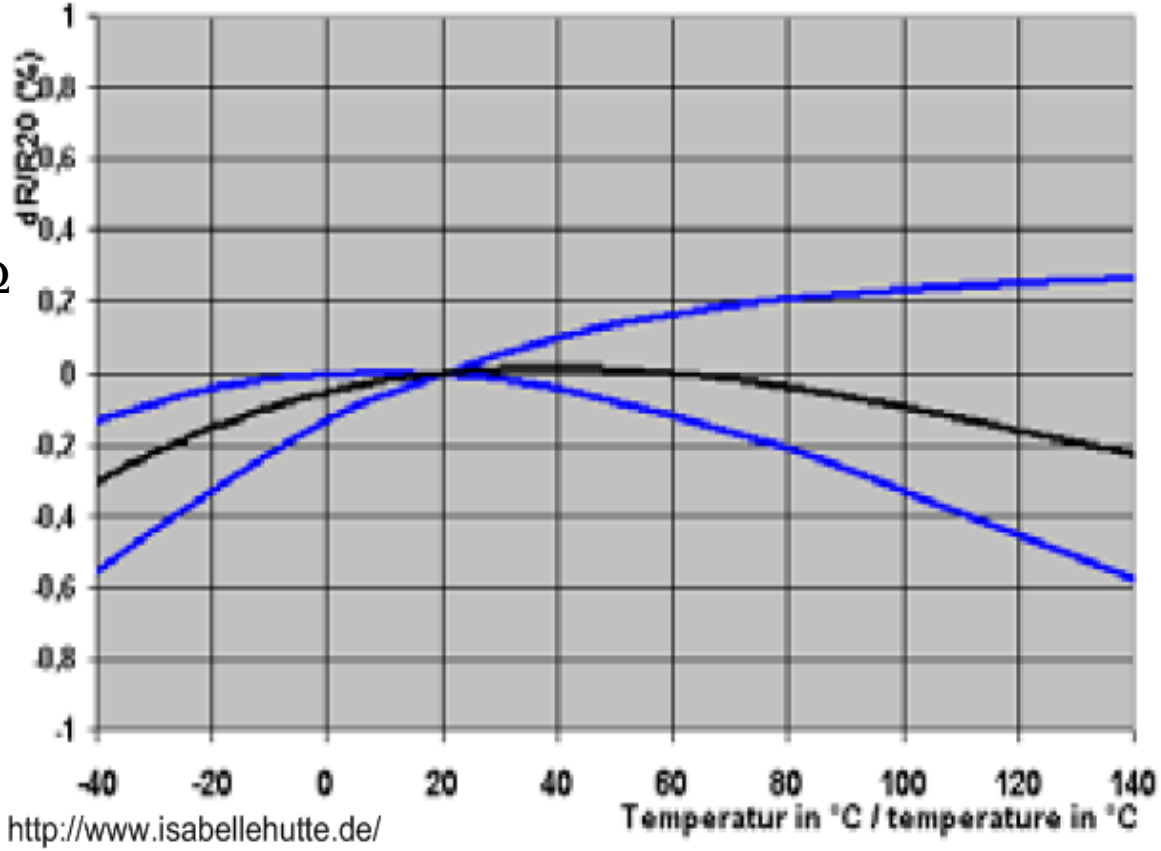
Voltage drop across shunt resistor is proportional to the amplitude of the current and frequency.

Current sensors - shunt resistor cont'd.

✓typical 60A shunt:
0.3mΩ, 3nH, 20ppm/°C,
great linearity

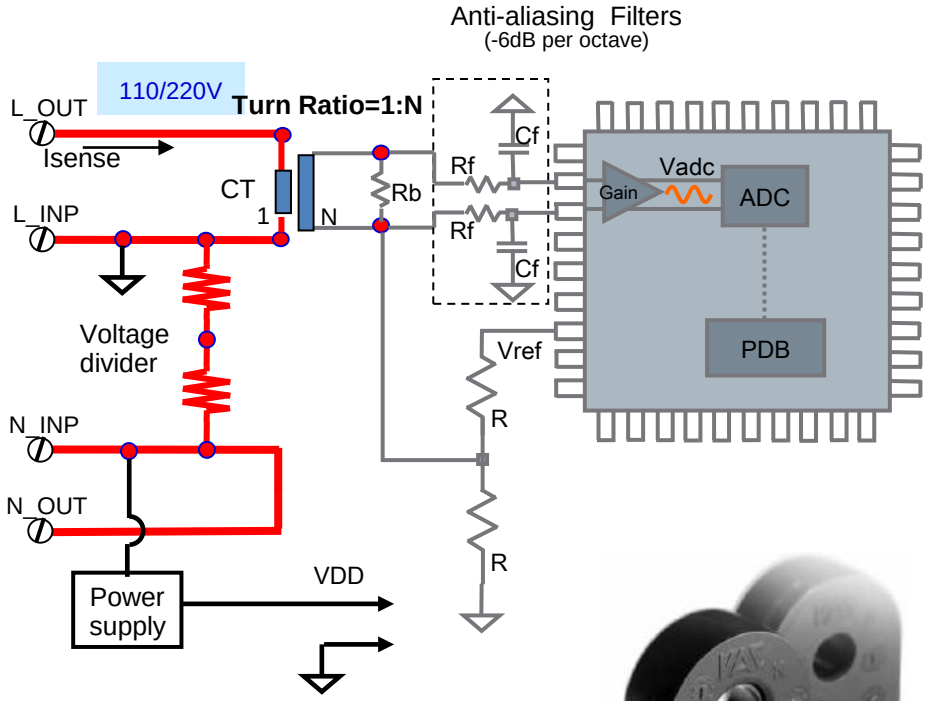
✖power consumption limitation
to 2W by EN470

✖2W / 60A^2 = 0.55mΩ -> .300mΩ
gives ~ 25mV max



http://www.isabellehutte.de/

Current sensors - current transformer



Pros:

- *Provides electrical isolation*
- *Current in secondary proportional to current in primary.*
- *Preferred for poly-phase meters*
- *Output voltage scaled to ADC input signal range*

Cons:

- *CT introduces phase error from 0.1° to 7.0°*
- *Phase shift depending on current and temperature*
- *Load must never be disconnected from secondary winding*
- *Iron core can saturate at current level beyond its rated current or at a large DC.*
- *Sensitive to magnetic tampering*
- *Expensive*

Mathematical description:

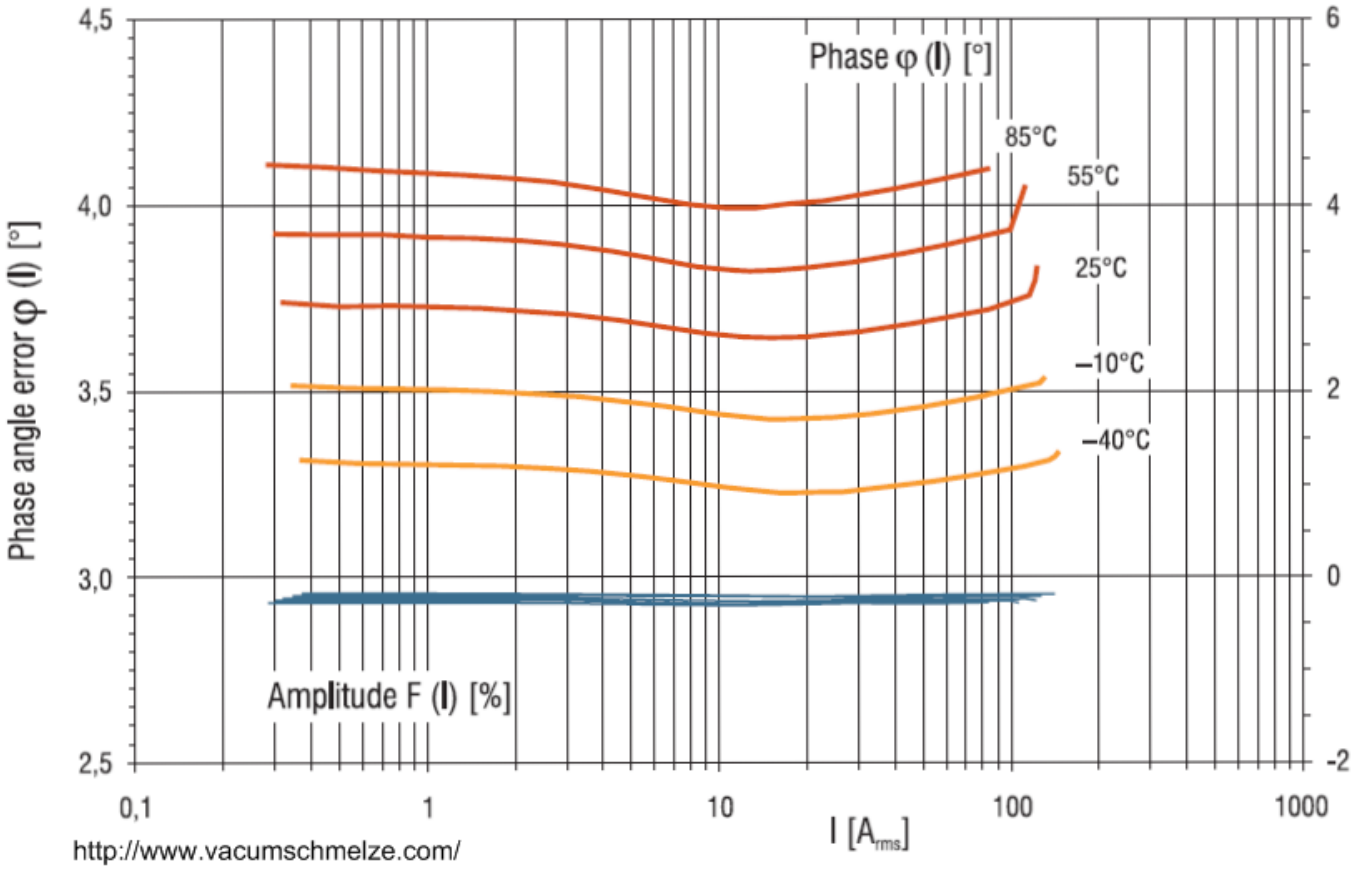
$$I_{SENSE} = \frac{(Vadc - \frac{Vref}{2})}{Gain * Rb * N}$$

by courtesy of
VACUUMSCHMELZE

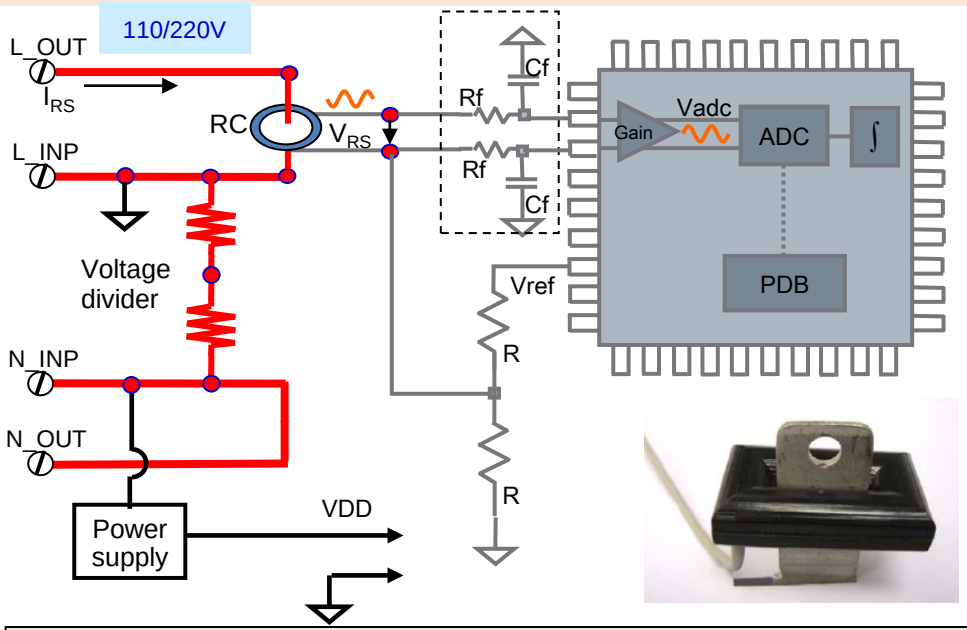
I_{SENSE}(A)	Ratio	$U_{SENSE}(V_{P-P})$
0.02	1:2500 Rb=12.5Ω	282.8uV
0.15		2.1mV
60		0.848V

Current sensors - current transformer

- ✓galvanic isolation
- ✓amplitude error is negligibly small
- ✖phase error is function of current nonlinear
- ✖typically 60A CT: phase error 4.42° 1:2500 ratio
- ✖ sensitive to DC and magnetic tamper.



Current sensors - current transformer



Pros:

- *Provides electrical isolation*
- *Capable of handling high current*
- *Low temperature drift*
- *Linear phase response*
- *No DC or high current saturation*
- *Immune to magnetic tampering*

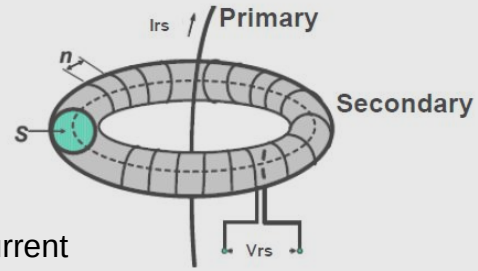
Cons:

- *Integration adds to extra circuitry (software load)*
- *Interference (far field) pickup - limited by design or shielding.*

Mathematical description:

$$V_R = K_R * Fr * I_R$$

$$Vadc = \frac{Vref}{2} + GAIN * V_R$$



where:

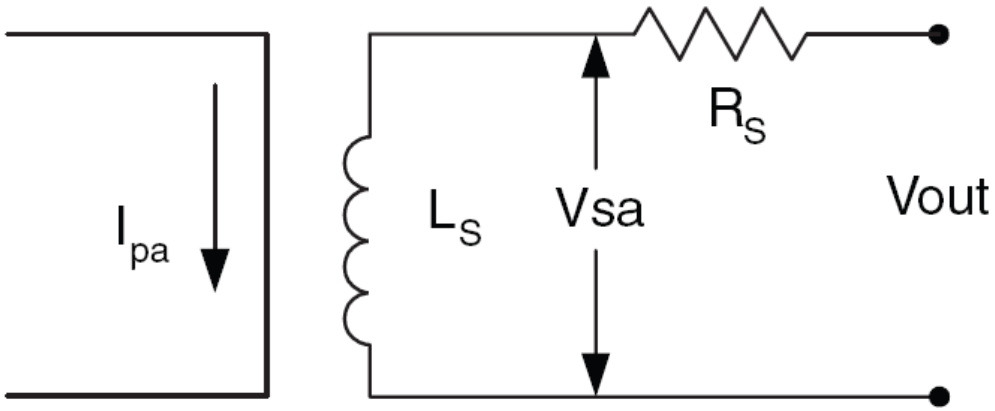
I_R = rated primary current
Fr = frequency of sinusoidal waveform
K_R = rotated transformer constant

I_{SENSE}(A)	F_r(μΩ/Hz)	U_{SENSE}(V_{P-P})
0.02	8.33 (PA3202NL)	23.56uV
0.15		176.71uV
60		70.7mV

The output voltage of the Rogowski coil is proportional to the time-differentiation (di/dt) of the current.

Current sensors - current transformer

- ✓output voltage proportional to the rate of change of current
- ✓typically 0.1 : 1000A, high linearity
- ✓galvanic isolation
- ✖ sensitive to electromagnetic noise
- ✖ -90°phase shift of output voltage to prim. current



$$Vsa = K_r F_r I_{pa} \qquad Fr << SRF$$

Accu.(%)	Kr(μΩ/Hz)	Ls(mH)	Rs(Ω)	SRF(Hz)
0.02	6.16	1.0	42.0	360k

Current sensors - comparison

Sensor Type	Shunt Resistor	Current Transformer	Hall-effect Device	Rogowski Coil
Cost	Very Low	Medium	High	Low
Linearity over measurement range	Very Good	Fair	Poor	Very Good
High current measuring capability	Very Poor	Good	Good	Very Good
DC/High current saturation	No	Yes	Yes	No
Power consumption	High	Low	Medium	Low
Output variation with temperature	Medium	Low	High	Very Low
DC Offset problem[(1)]	Yes	No	Yes	No
Saturation and hysteresis	No	Yes	Yes	No

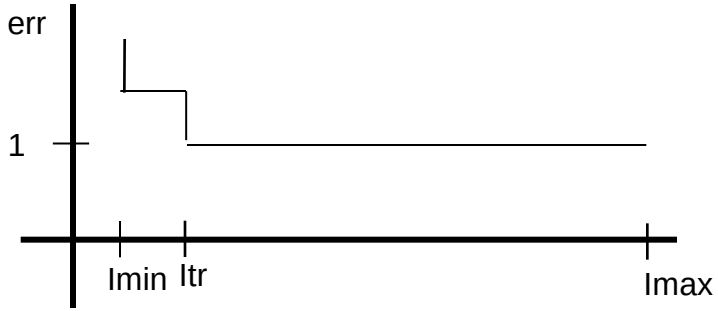
http://www.pulseelectronics.com/docs/graf/smart_grid_white_paper.pdf

EN 50470-3 static power meter accuracy and dynamic range

- dynamic range @ accuracy required
  - Common static power meter Class B: (5)60A requirements

Class	Ireference [A]	Imaximum [A]	Itransitional [A] Itr = Iref/10	I minimum [A] Imin=0.5*Itr	Accuracy [%] <imin; Itr>	Accuracy [%] <Itr; Imax>
A	5	100	0,5	0,25	2,5	2
B	5	100	0,5	0,25	1,5	1
C	5	100	0,5	0,15	1	0,5

B class:
Imax : Imin = 100 : 0,25 → **400** : 1 (*DR*)
accuracy **1,5%** i<Itr, 1% i>Itr
C class:
Imax : Imin = 100 : 0,15 → **666** : 1 (*DR*)
accuracy **1%** i<Itr, 0.5% i> Itr



ANSI C12.20 power meter accuracy and dynamic range

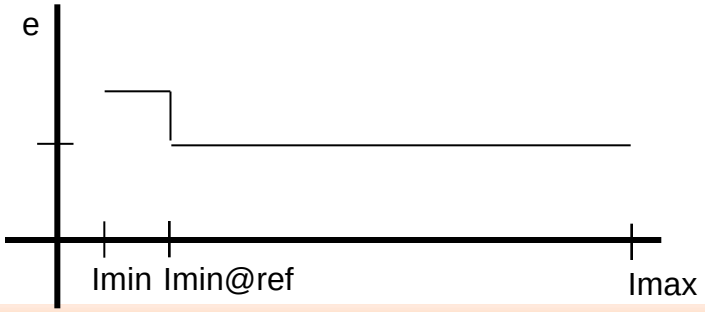
- dynamic range @ accuracy required
  - ANSI C12.20 power meter Class 0.2: (30)200 requirements

	Current in Amperes		Maximum error deviation [%]	
	Current Class		Accuracy class	
Conditions	100	200	0.5	0.2
Starting current	0.1	0.1	-	-
(1) Imin	1	2	±1.0	±0.4
(2) Imin@ref	**1.5**	**3**	**±0.5**	**±0.2**
(3)	3	6	±0.5	±0.2
(4)	10	20	±0.5	±0.2
(5)	15	30	±0.5	±0.2
(6)	30	60	±0.5	±0.2
(7)	50	100	±0.5	±0.2
(8)	75	150	±0.5	±0.2
(9)	90	180	±0.5	±0.2
(10) Imax	**100**	**200**	**±0.5**	**±0.2**

dynamic range out of table Imax :

Imin@ref = 200 : 3.0 → 66.6 : 1 (*DR*)

accuracy required for class 0.2 meter 0.2% (*err*)



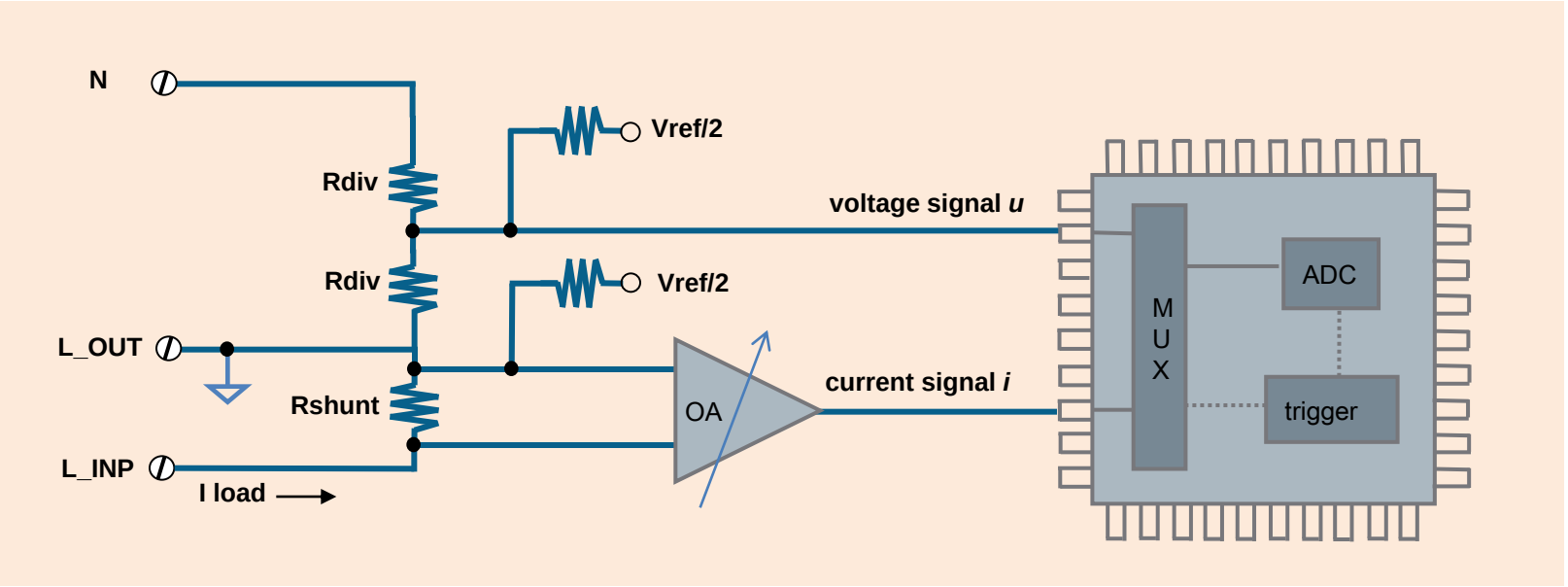
Phase voltage sensing

- No special conditioning needed typically very low dynamic range required max. 1:3
- Resistor network
  - minimal phase shift error introduced
  - overvoltage and over current susceptibility
  - LPF has typically very high impedance
- Voltage transformer
  - usually used for half-direct measurement (high voltages)

Single, two and three phase topologies

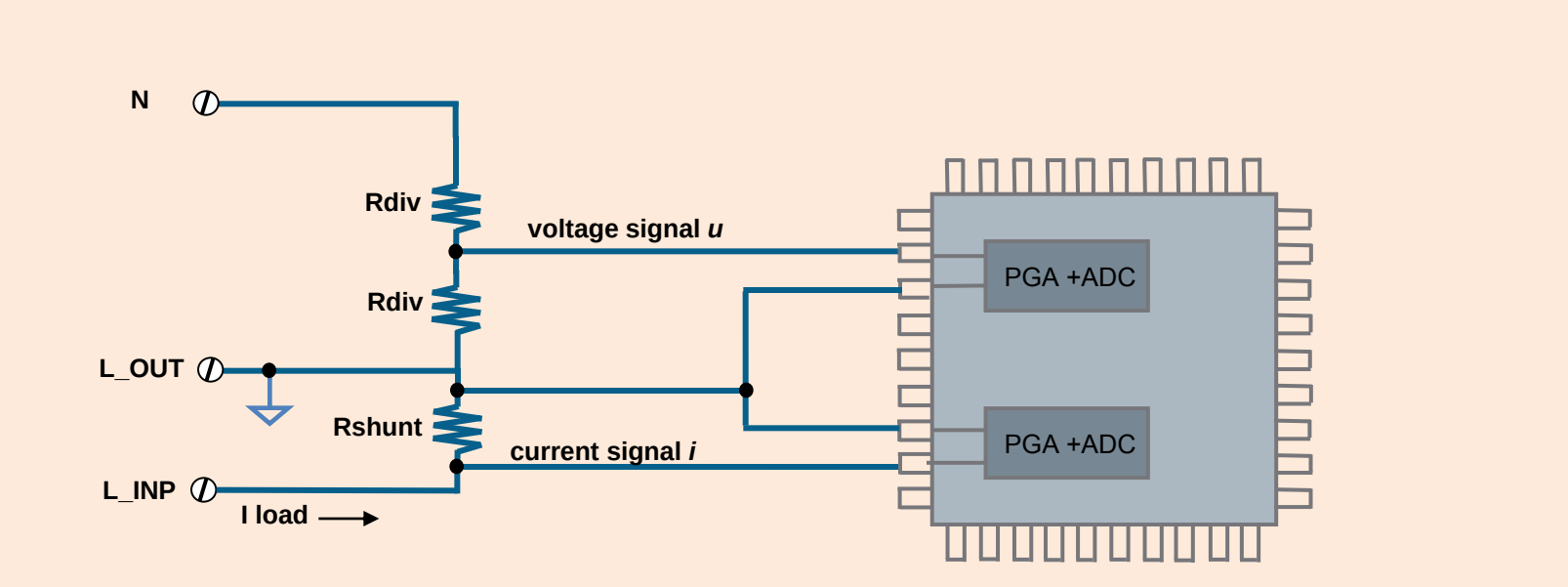
- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- current, voltage sensors used in static meters
- **single, two and three phase topologies**
- energy calculation algorithms active and reactive energy
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- existing MCU overview

Static 1-ph. shunt based meter ADC w/out PGA



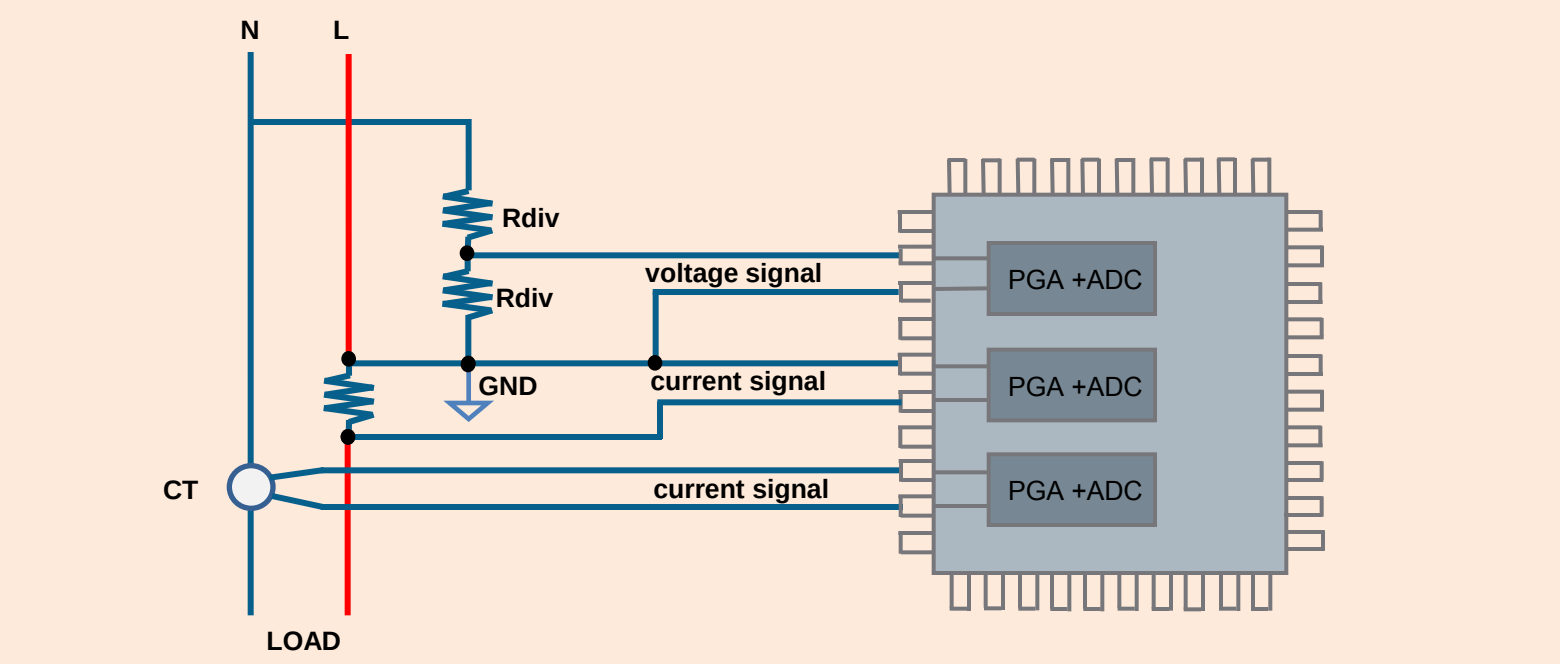
- meter GND lies on the phase L
- if ADC doesn't have PGA, external OA needed
- differential sensing / amplifying is expensive
- the most of single phase meters are shunt based - shunt in live L
- DC bias needed

Static 1-ph. shunt based meter, ADC with PGA



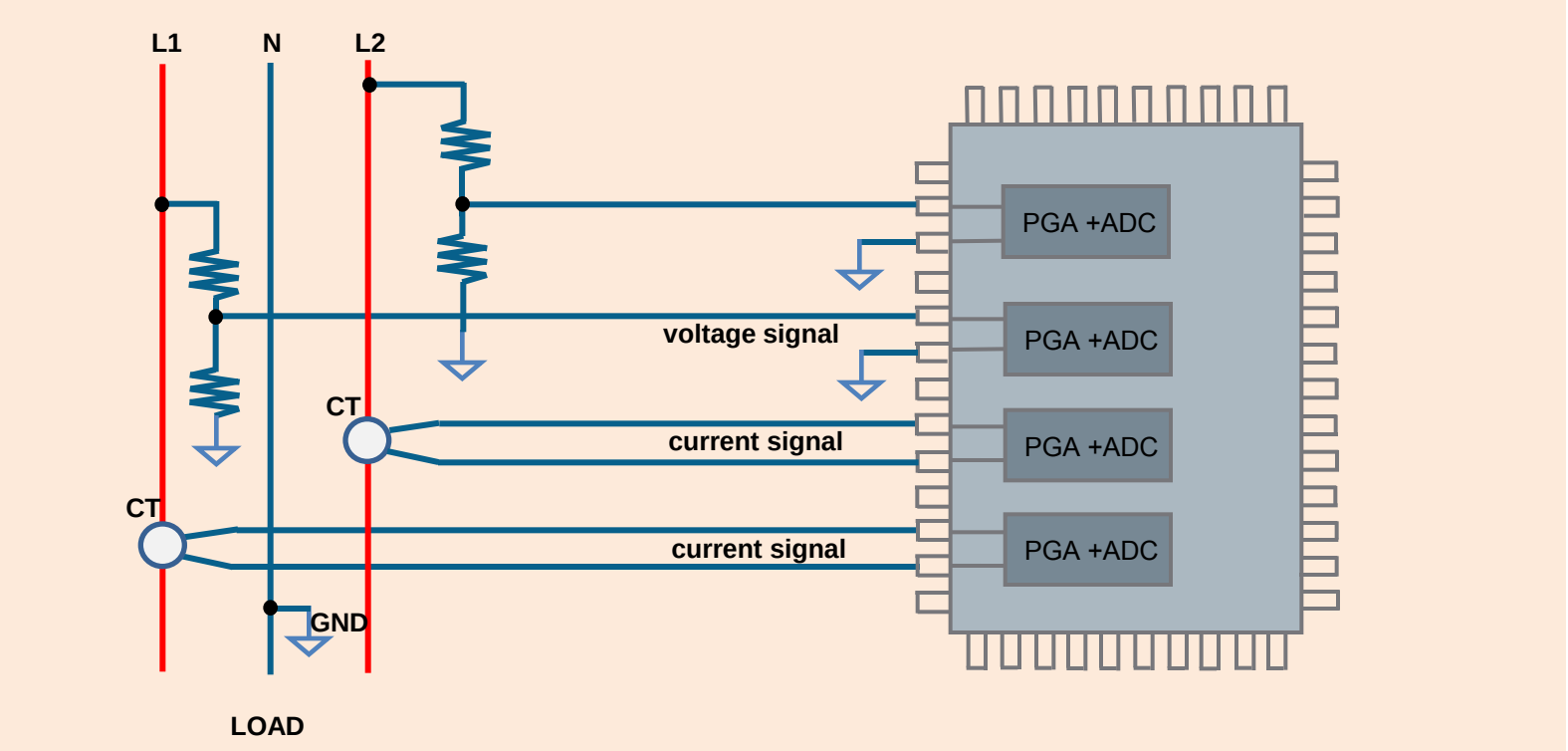
- meter GND lies on the phase L
- differential sensing possible
- PGA must be able to work with negative voltages
- the most of today's single phase meters use this topology

Static 1-ph. shunt based ADC with neutral sub-metering



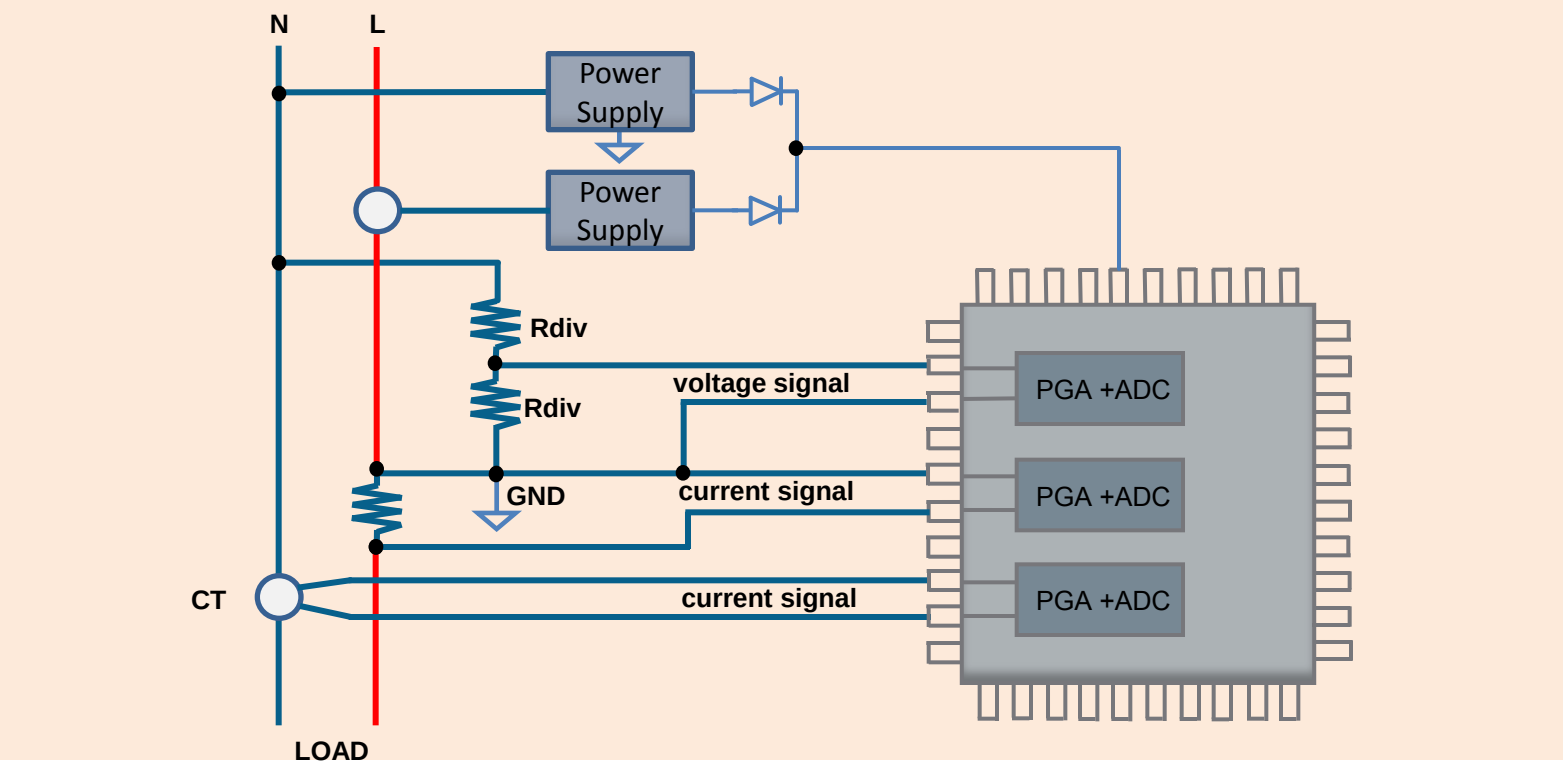
- meter GND lies on the phase L
- current sensed on shunt resistor and on current transformer (CT)
- prevents tampering - double feeding meter

Static 1-ph. shunt based ADC w/out PGA



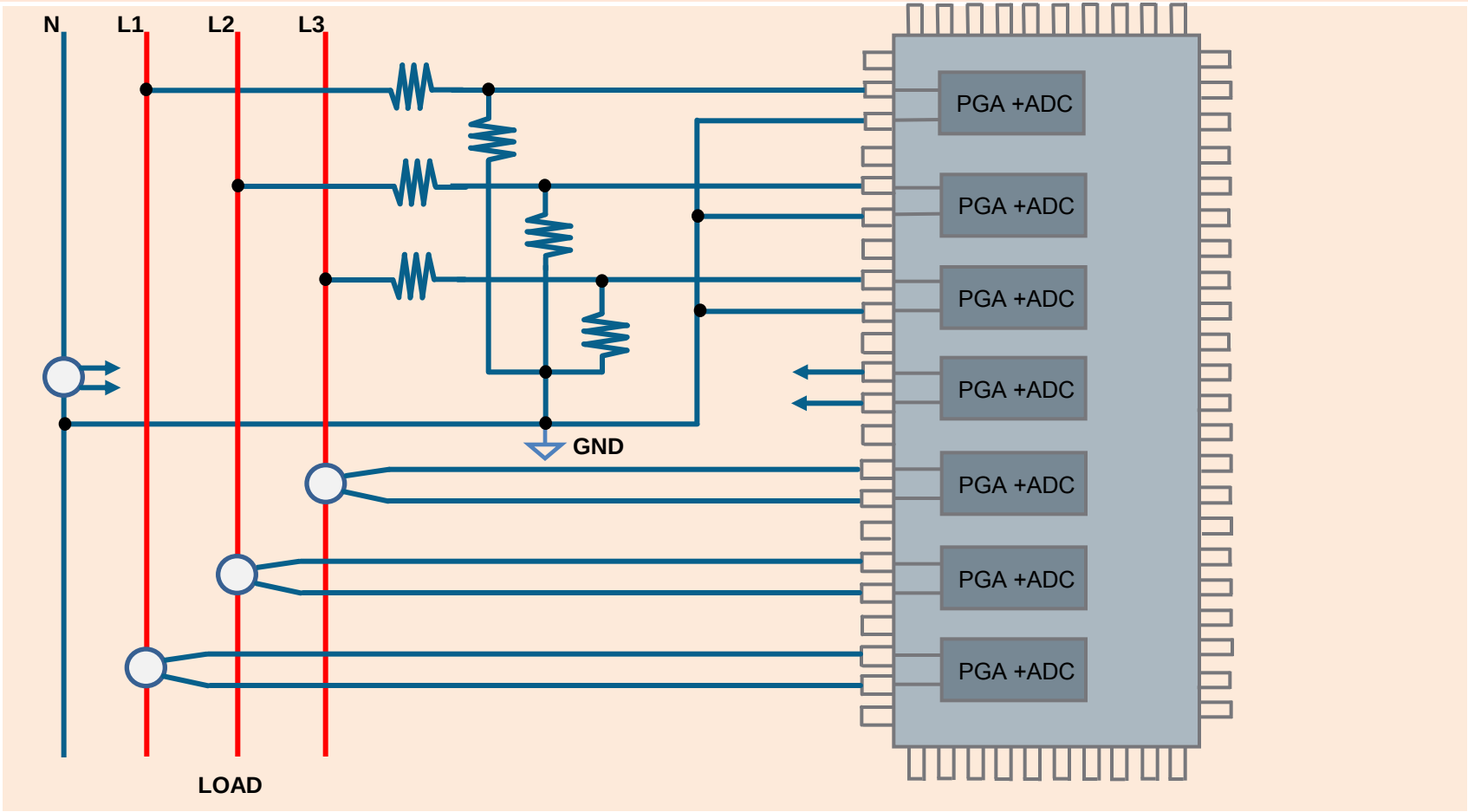
- Form-12S Electricity Meter - US, JAPAN
- meter GND lies on the neutral N
- CT must be used to isolate from phase voltage

Static 1-ph. CT + Shunt based power meter with safety power supply



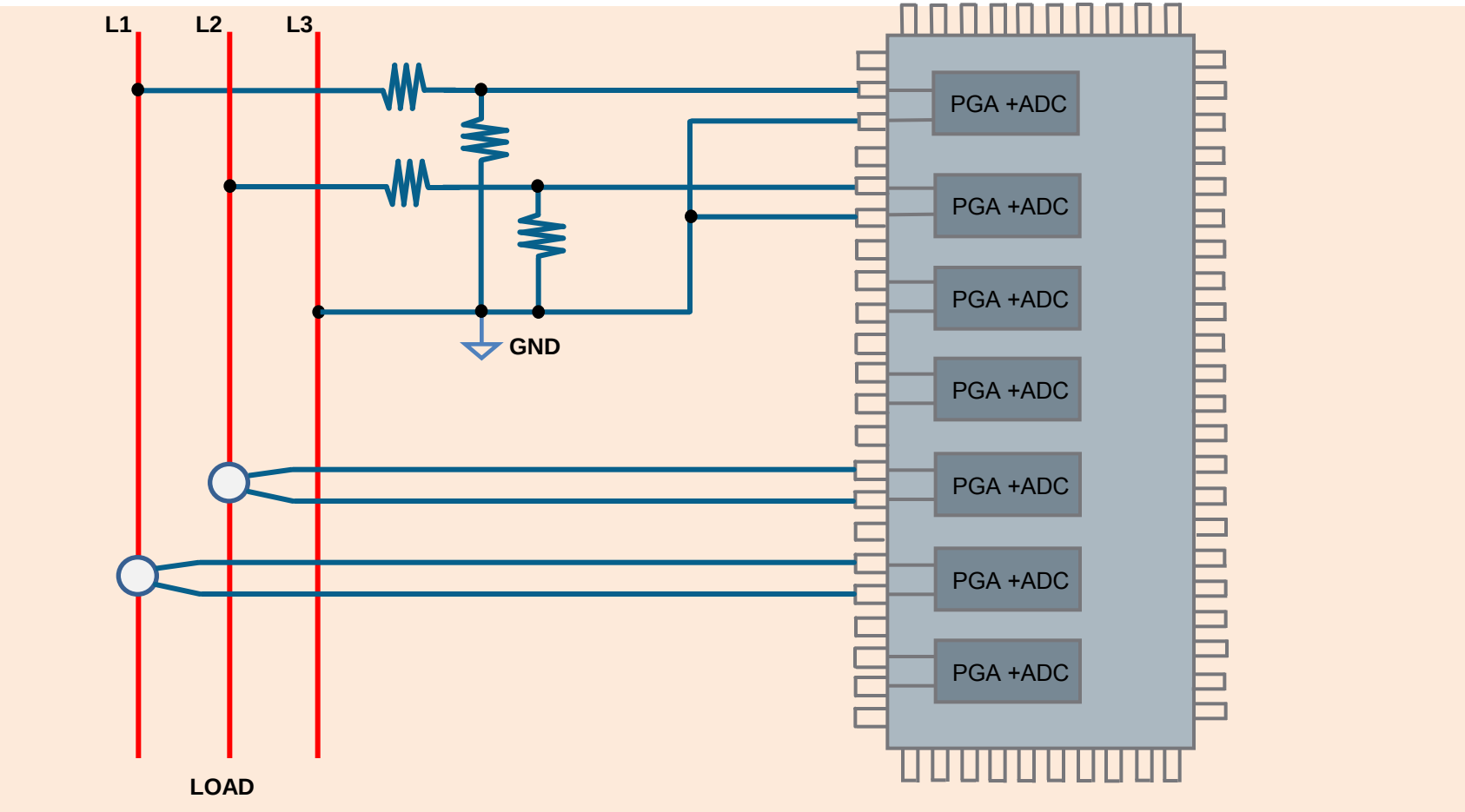
- meter GND lies on the phase L
- current sensed on shunt resistor and on current transformer (CT)
- prevents tampering - double feeding meter + adds power supply when missing neutral

Static 3-ph. shunt based ADC with PGA



- 3P4W - 3 watt meters

Static 3-ph. shunt based ADC with PGA



- 3P3W - 2 watt meters

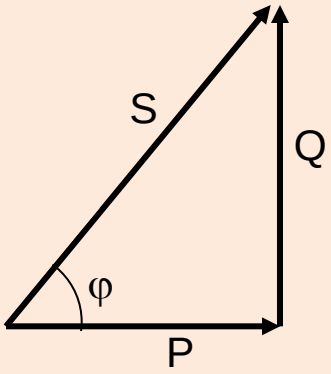
Energy calculation algorithms active and reactive energy

- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- current, voltage sensors used in static meters
- single, two and three phase topologies
- **energy calculation algorithms active and reactive energy**
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- existing MCU overview

Power - Calculation algorithms
Total, active and reactive power

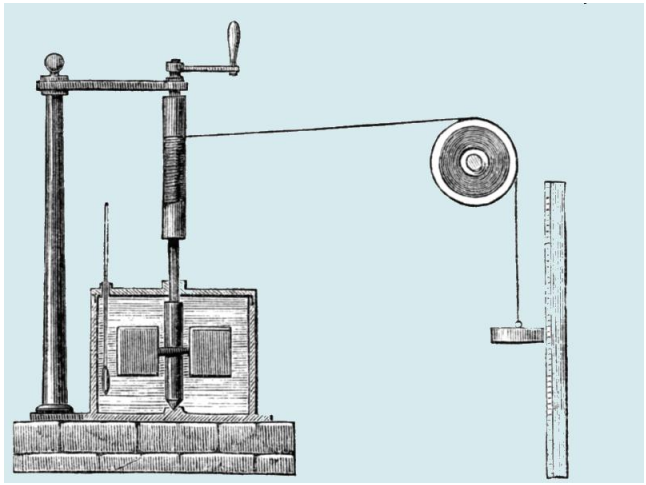
- common utility system is based on "**total apparent power S_{tot}**" [VA] load to be served
- "**total apparent power**" is product of the RMS voltage and RMS current
- "**active power**" [W] equal voltage times the working component of the current
- **"reactive power"** [VAR] is equal to the voltage times the magnetizing (reactive) current
- **"apparent power**" [VA] is vector sum of active and reactive power
- in pure sinusoidal system with no higher harmonics the **apparent power** equals to **total apparent power**
- once harmonics are encountered in system vector sum **loose accuracy**

$$S = \sqrt{P^2 + Q^2}$$



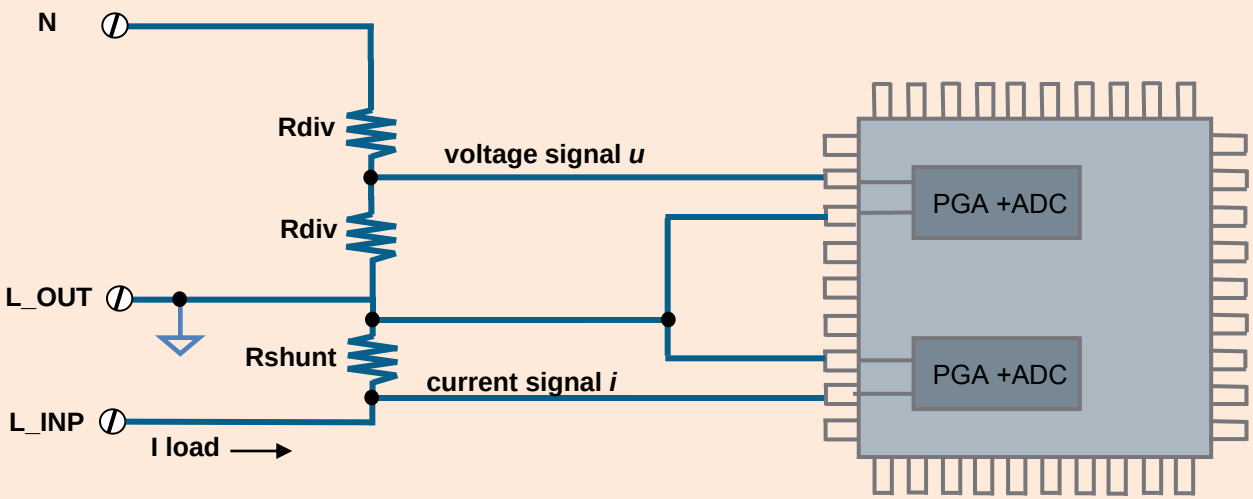
$$S_{tot} = \sqrt{S^2 + D^2}$$

Active power and active energy calculation equation



- watts equal volts times the working component of the current
- active power $$P = \frac{1}{T}\int_0^T u(t)i(t)dt$$
- and active energy $$W = \int_0^\infty u(t)i(t)dt$$
- in discrete time
  $W = \sum_{k=1}^{\infty} U_k I_k$ where U_k, I_k are instantaneous values
- as sum of harmonic
  $P = \sum_{k=1}^{\infty} U_k I_k \cos(\varphi_k)$ where U_k, I_k are RMS values of the k^{th} harmonic and φ_k is angle in between
- Those equation is **correct** in AC and DC circuits and **with or without harmonics**

Active Power Calculation versus signal errors



- U_0 , I_0 and φ_{ie} are considered as **signal error**
- measured current signal
  - I_0 composed of PGA offset, ADC offset
  - φ_{ie} *is* introduced on shunt inductance, amplifier, φ_L on reactive part of the load

$$i = I_0 + g * i \sin(\omega t + \varphi_L + \varphi_{ie})$$

- measured voltage signal
  - U_0 composed of ADC offset
  - φ_{ue} phase error is given on resistors ESR, ESL

$$u = U_0 + g * u \sin(\omega t + \varphi_{ue})$$

Active Power Calculation versus signal errors

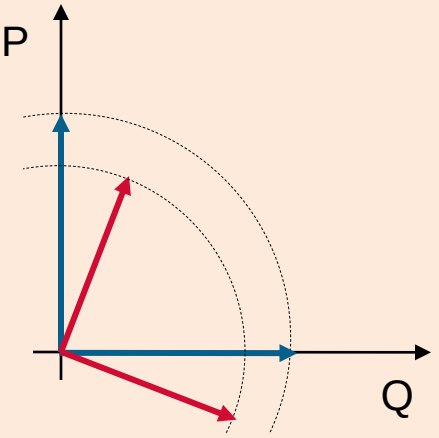
- **phase error φ_e** causes **bad power factor** metering
- **phase error φ_e** cause bad active power calculation for **non pure active** loads (reactive part included)

$$W = \int_0^{\infty} u(t)i(t)dt = \int_0^{\infty} u\sin(\omega t + \varphi_{ue})i\sin(\omega t + \varphi_L + \varphi_{ie})$$

- subtract φ_{ue} from signals $\varphi_e = \varphi_{ie} - \varphi_{ue}$

$$W = \int_0^{\infty} u(t)i(t)dt = \int_0^{\infty} u\sin(\omega t)i\sin(\omega t + \varphi_L + \varphi_e)$$

power vectors **pure active load**
good compensated
bad compensated



phase error φ_e might be removed by:

- phase compensation in hardware – additional components
- time shifted ADC sampling – samples are taken in time equal to φ_e
- for large phase shift (CT) we need to move samples!
- by software for example using digital filter

$$y[n] = x[n] + b\,x[n-1]$$

Active Power Calculation versus signal errors - offset

- ***i(t), u(t)*** signals **error DC offset U_0 , I_0** introduced in AFE cause an **error** in the **active power** calculation
- mains **current** may have DC component – half wave rectifier
- the mains **voltage** shouldn't have DC component

$$W = \int_0^{nT} u(t)i(t)dt = \int_0^{nT} \left(U_0 + u\sin(\omega t)\right) * \left(I_0 + i\sin(\omega t)\right) dt$$

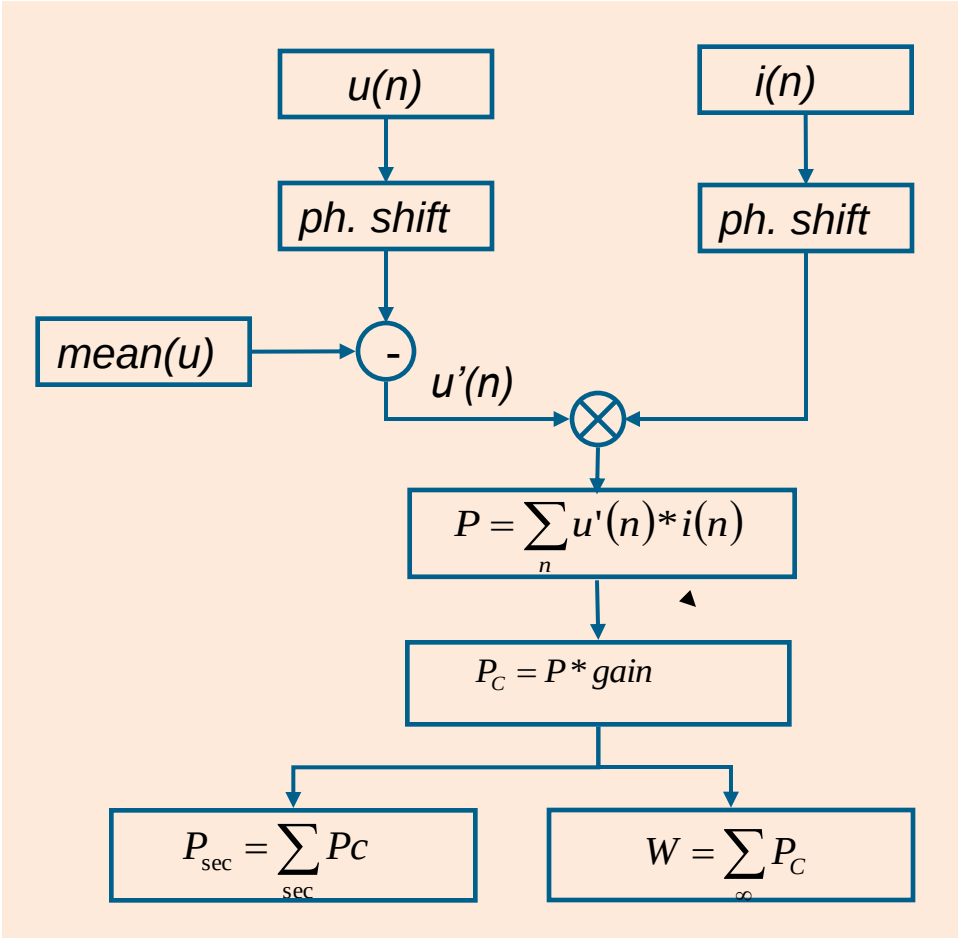
$$W = \int_0^{nT} I_0 U_0 + I_0 u\sin(\omega t) + U_0 i\sin(\omega t) + i\sin(\omega t) u\sin(\omega t)\, dt$$

- lets **assume that there isn't direct voltage on the mains** $U_0 = 0$
- **integral of sin per one period** is zero
- then we can simplify equation to

$$W = \int_0^{nT} i\sin(\omega t) u\sin(\omega t)\, dt \text{ and for discrete form } \sum_0^{nk} u[n] * i[n]$$

Active Power Calculation Removing U_0 from measured signal

- hw solution
  - higher component cost
  - differential ADC converter
  - sensitive to thermal drift
  - sensitive to aging
- subtract fixed offset value from samples
  - easy to implement, low CPU time
  - sensitive to thermal drift,
  - sensitive to aging

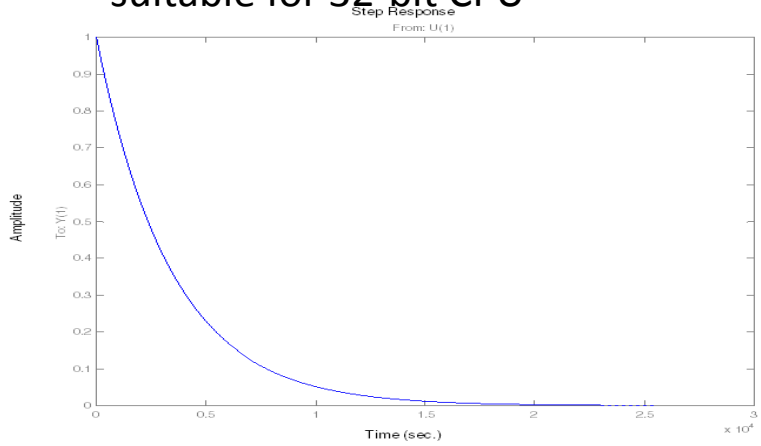


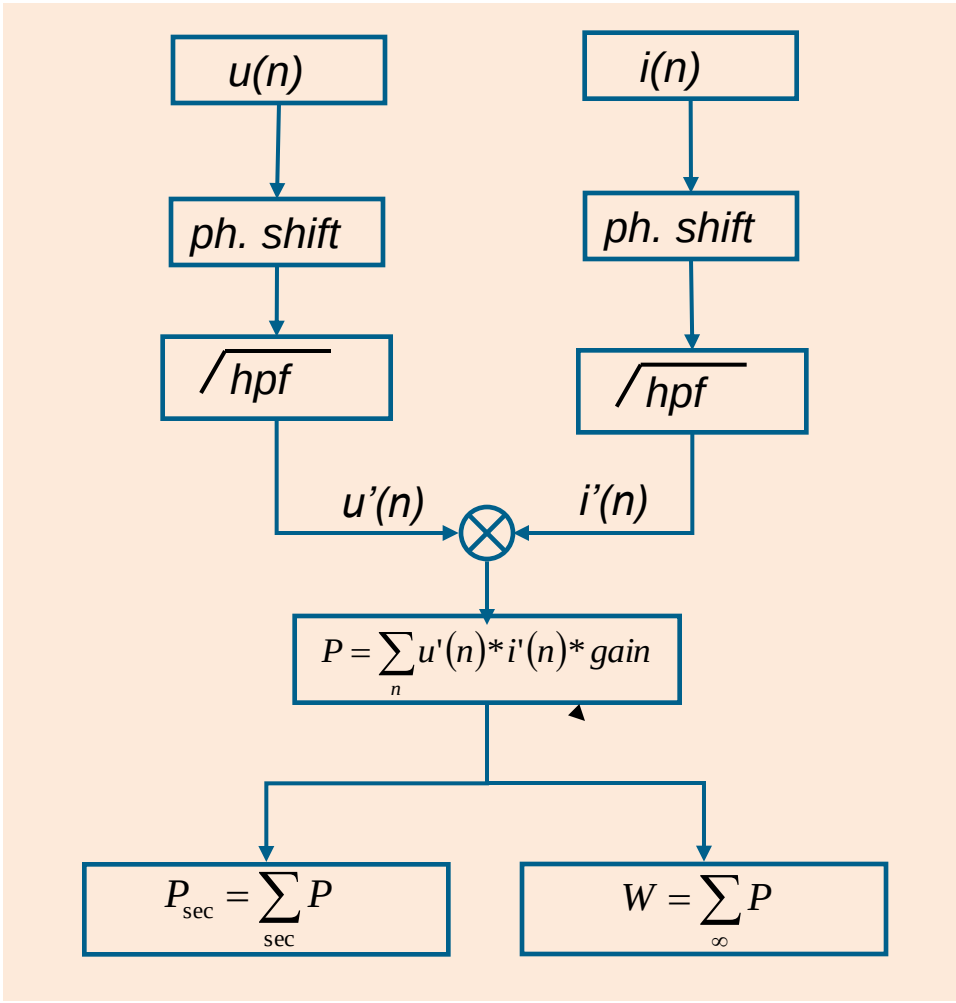
Active Power Calculation Removing U_0 from measured signal

- digital filter
  - longer settling time
  - higher CPU load
  - must be applied on both voltage and current
  - simple Butterworth filter requires 3xMAC per sample

$$y = 0.998x_n - 0.998x_{n-1} + 0.997y$$

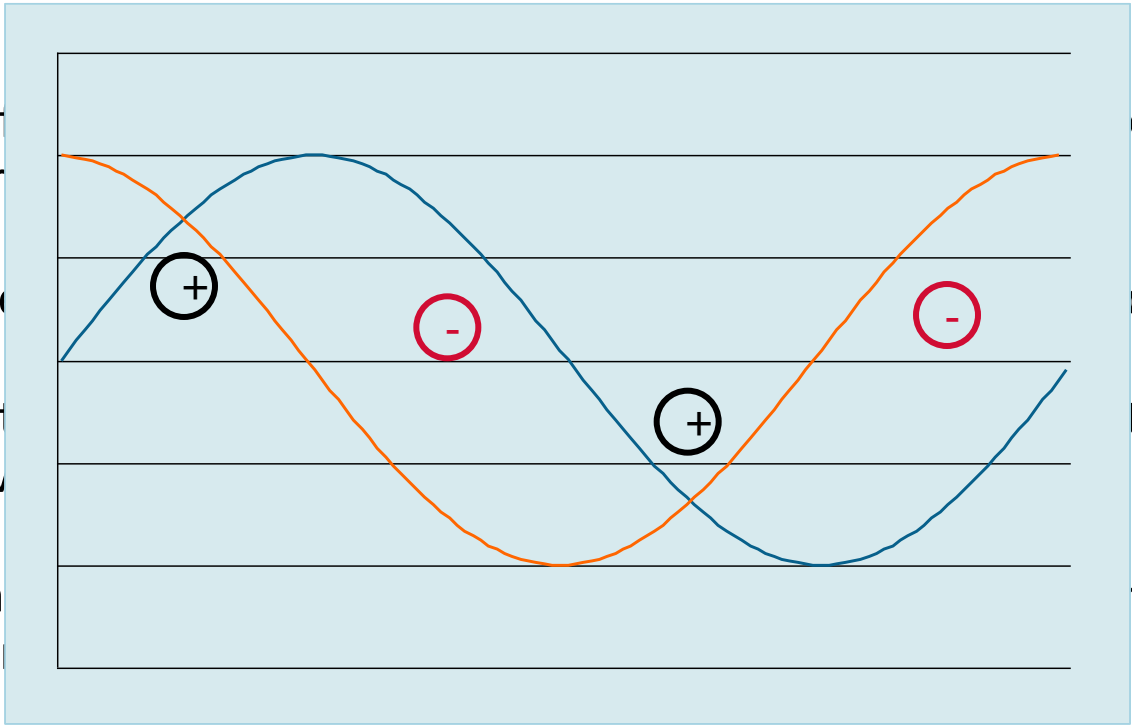
  - suitable for 32-bit CPU





Reactive power and reactive energy calculation

- purely reactive load cause the voltage and current are 90 degrees out of phase
- for half o sitive, but on the other
- in averag ck
- it is easy t tage and current w
- if non-sin n methods give diffe
- frequency changes causes measurement error as well



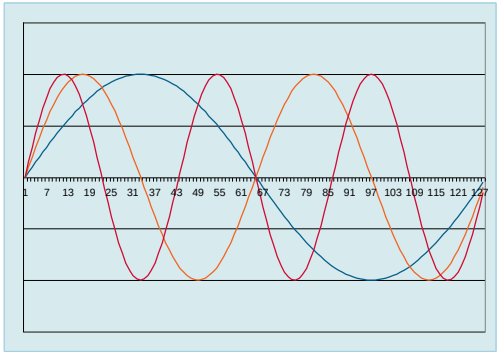
Reactive power and reactive energy calculation

- Reactive power **S [VAr]** equal volts times the magnetizing (reactive) component of the current

- magnetizing component of the current lags the working component by 90°, this quantity could be read by a wattmeter if the voltage applied to the wattmeter could be displaced by 90° to bring it in phase with the magnetizing current

- in time domain $$VAR = \int_0^{\infty} u(t-90^{\circ})i(t)dt$$

- in frequency domain

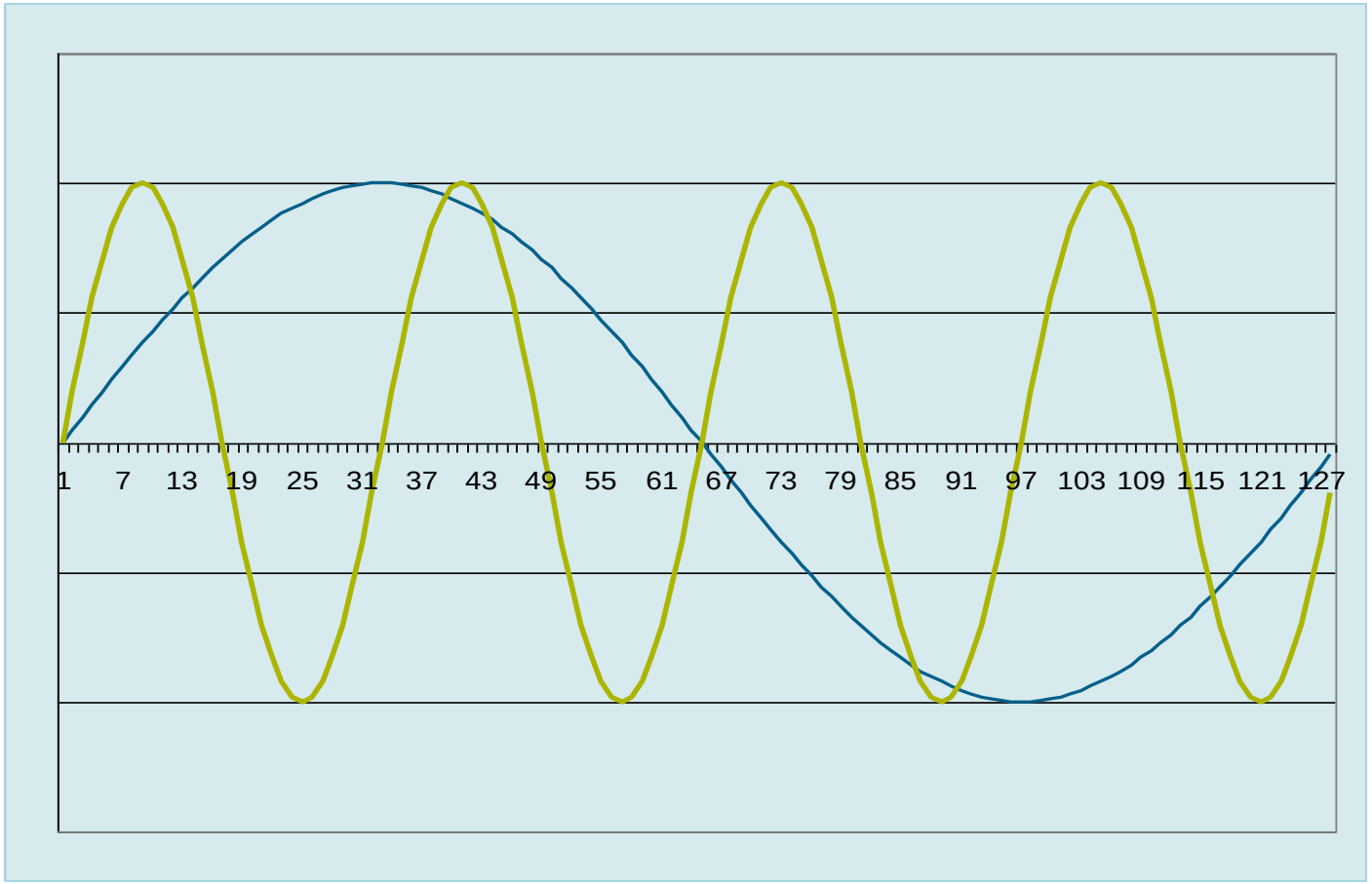


$$VAR = \sum_{k=1}^{\infty} U_k I_k \sin(\varphi_k)$$ where U_k, I_k are RMS values of the k^{th} harmonic and φ_k is angle in between

Reactive power and reactive energy calculation

- Only same harmonics are creating power

$$VAR = \sum_{k=1}^{\infty} U_k I_k \sin(\varphi_k)$$



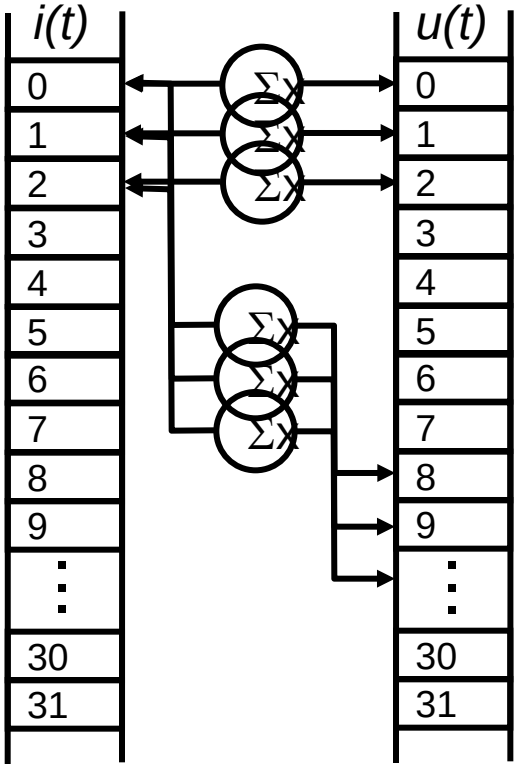
Reactive Power calculation time shift method

- **fixed time delay** that is equivalent to 90° of the fixed fundamental frequency is applied prior to the multiplication

- suppose we have 32 samples per one line period then 8 samples ~ 90° of fundamental frequency

$$Q_{period} = \sum_{k=0}^{31} U_k I_{k-8}$$

- if line frequency varies about its average an angle varies as well
  0.1%Δf ~ 0.09°~0.6% Q_{err}
- harmonics are delayed inaccurate
  8 samples ~ 180° of 2nd harmonics
  8 samples ~ 270° of 3rd harmonic



Methods of reactive power calculation – adjusted time shift

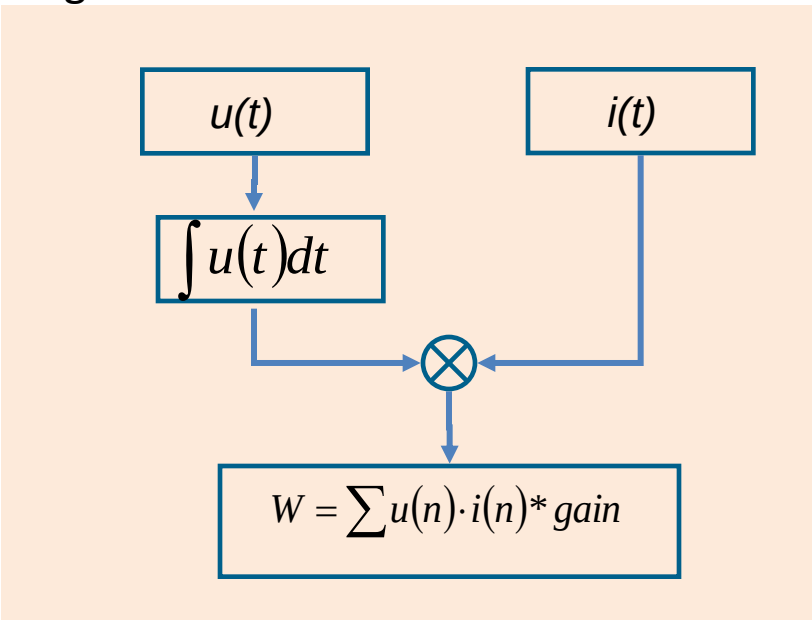
- **adjusted time delay** that is equivalent to 90° of the **actual** fundamental frequency is applied prior to the multiplication
- line frequency is tracked and sampling rate is adjusted to be synchronous
- error of the line frequency disappear
- **SAR** 16-bit ADC converter with **PDB is suitable** for this method
- **Sigma – Delta** can't change sampling rate precisely
- **harmonics** are **inaccurate** delayed

Methods of reactive power calculation – integration, derivation

- integration or derivation is employed on voltage or current prior to multiplication process
- fundamental frequency amplitude is proportional to mains frequency
- method affects harmonics making them smaller or large
- error is proportional to the harmonic
- second harmonic integration, derivation

$$\int \sin(2\omega t)dt = -\frac{\cos(2\omega t)}{2\omega}$$

$$\frac{d}{dt}\sin(2\omega t) = 2\omega\cos(2\omega t)$$

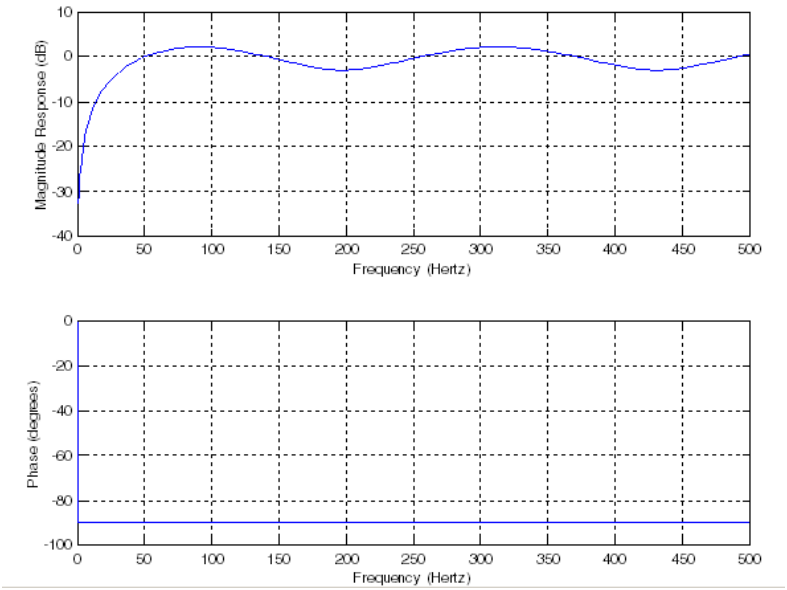


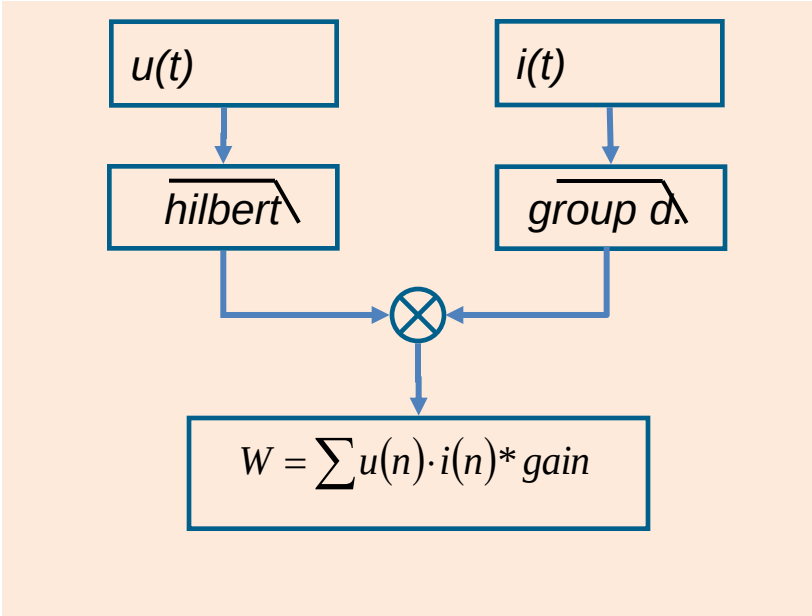
Methods of reactive power calculation – filters

- signal may be shifted using different kind of FIR or IIR filters
- magnitude / phase response sensitive to line frequency

  must be compensated
- higher CPU workload Hilbert filter

  64-bit implementation of 39th-order FIR filter, group delay, mul takes like 3000cycles on ARM M0+ core



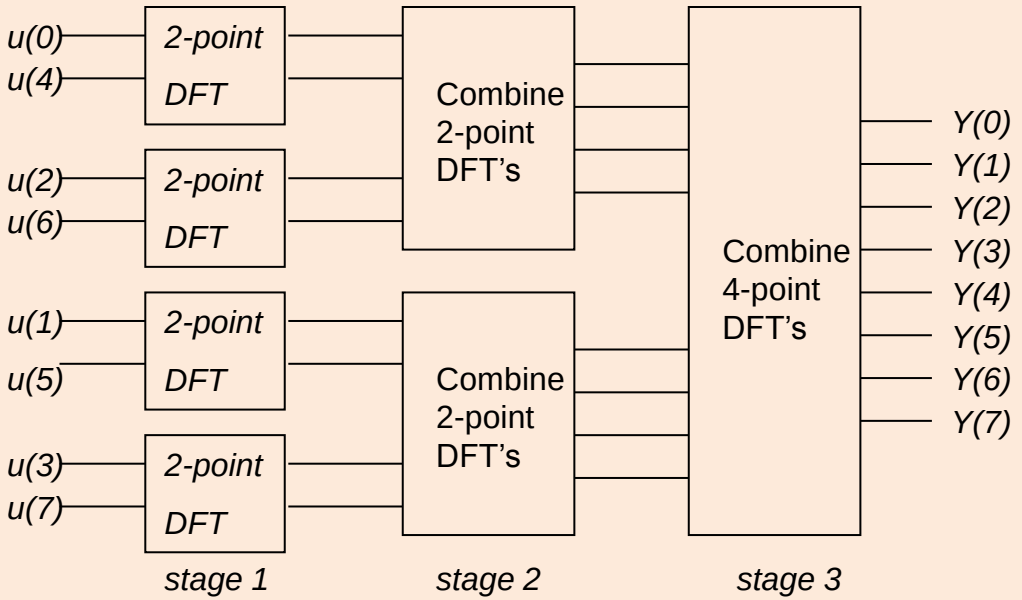


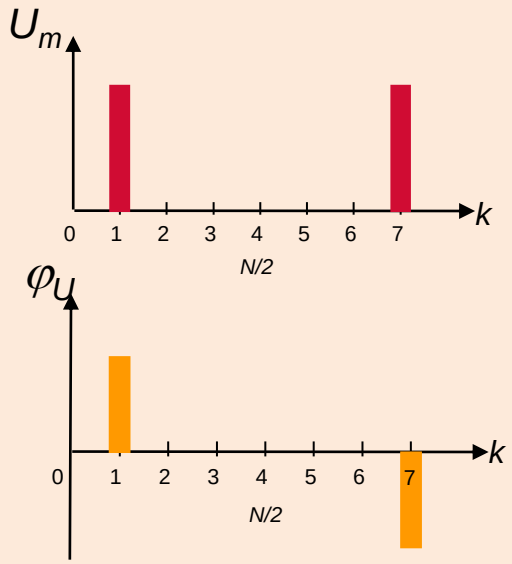
Methods of reactive power calculation – frequency domain

- signals *u(t), i(t)* are transformed to their corresponding harmonics representation by FFT (Radix-2 FFT)

input signal: *u(n), n = 1..N; N=8* output signal

$$U'(k) = \sum_{n=0}^{N-1} u(n) e^{-\frac{2\pi i}{N} nk}$$

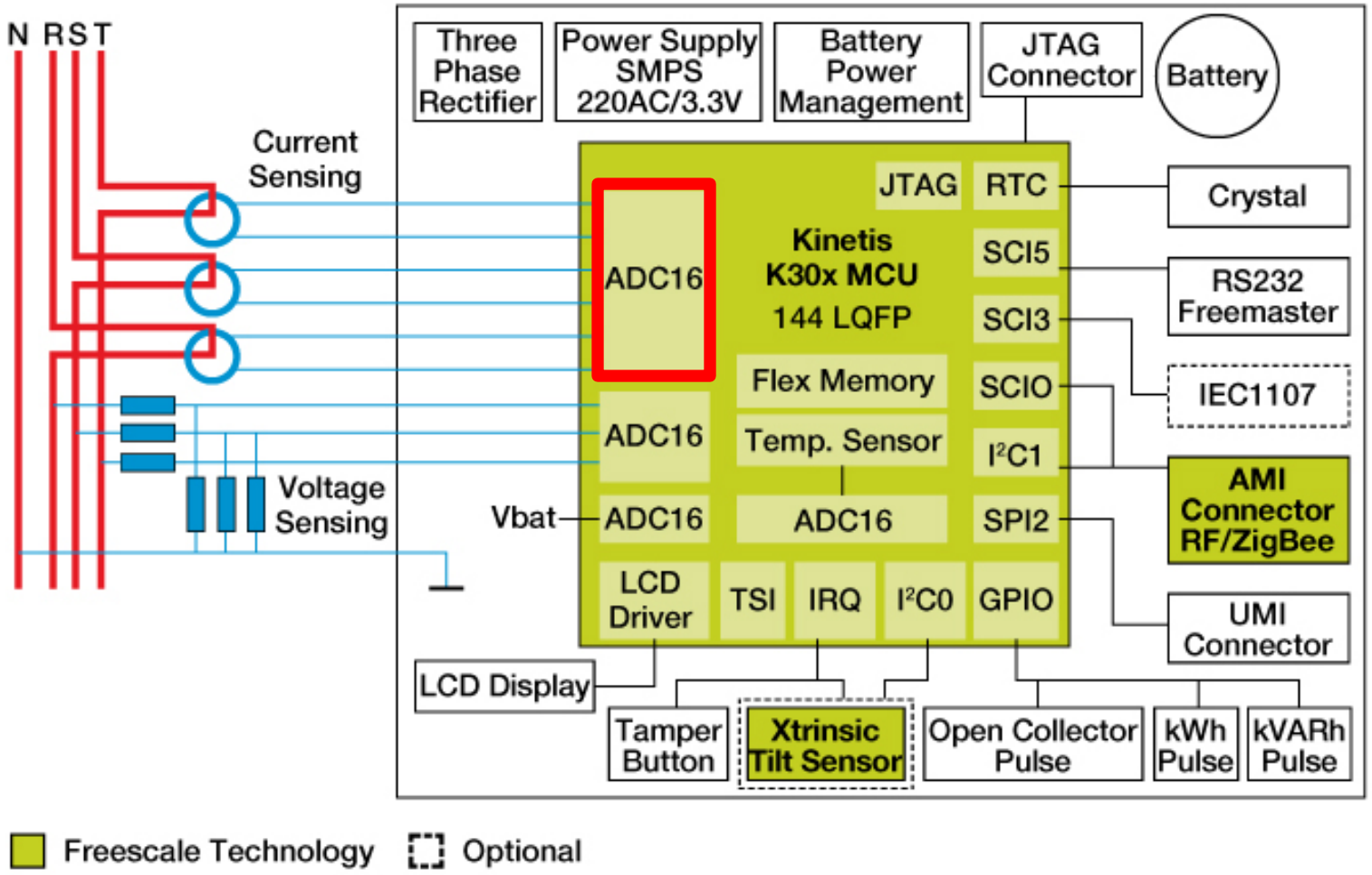




Microcontroller requirements ADC, DAC, tampers, RTC, CPU

- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- current, voltage sensors used in static meters
- single, two and three phase topologies
- energy calculation algorithms active and reactive energy
- **microcontroller requirements ADC, DAC, tampers, RTC, CPU**
- existing MCU overview

Single phase power meter block diagram



ADC key parameters

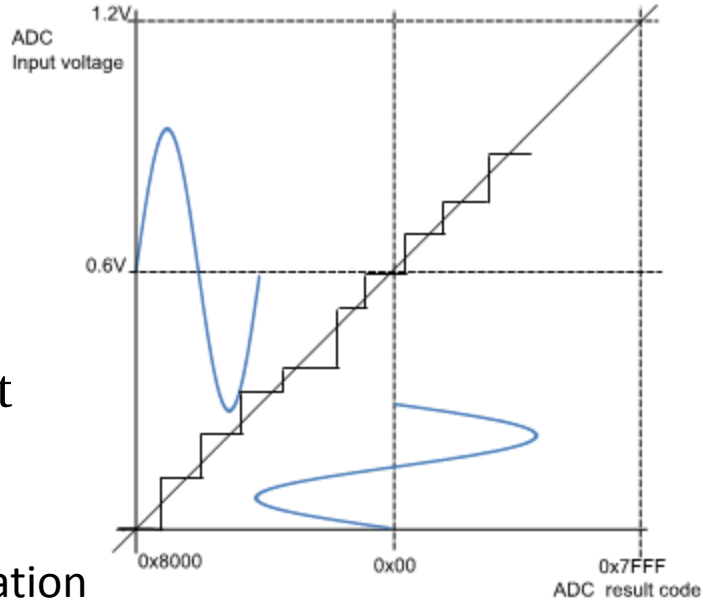
What are key ADC parameters for metering?

many parameter in the ADC specification ENOB, Resolution, SINAD etc. are making mess in the decision process

- **ADC RESOLUTION:**

$$ENOB = \frac{\ln(1/DR * err)}{\ln(2)}$$

$$ENOB = \frac{\ln(1/DR * err)}{\ln(2)} = \frac{\ln(1/666 * 0.01)}{\ln(2)} = 16\,\text{Bit}$$



- LINEARITY is essential for accurate metering application
- Sigma-Delta ADC is linear by its definition!
- White input noise is removed by oversampling

Sampling frequency and anti-alliasing

- the most of energy in first harmonic, by regulation 5th harmonic 300 (250)Hz is req. to be measured

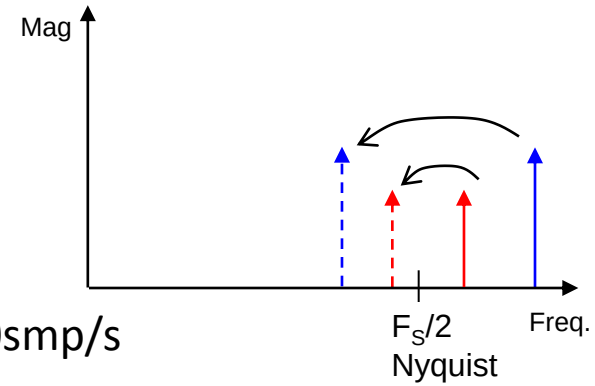
- due to recent load change (SMPS, fluorescent lamps, motor inverter) some energy placed up to 13th harmonics

- IEC calls for 21st harmonic today, some manufacturers expressed interest in 64th harmonic 21th harmonic gives Nyquist frequency

  21*60(50)*2 = 2520(2100) smp/sec

  this leads to ~8ksmp/sec

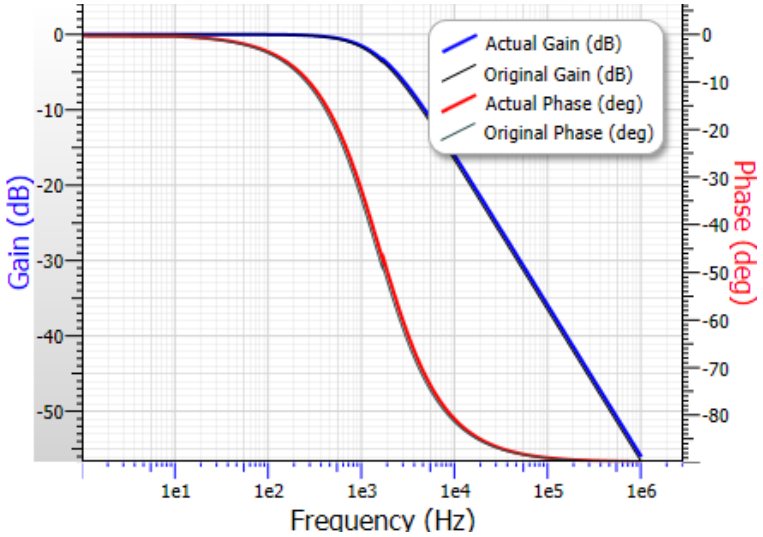
- today's sampling frequency manufacturer convention is around 30 smp/mains period ~1500smp/s



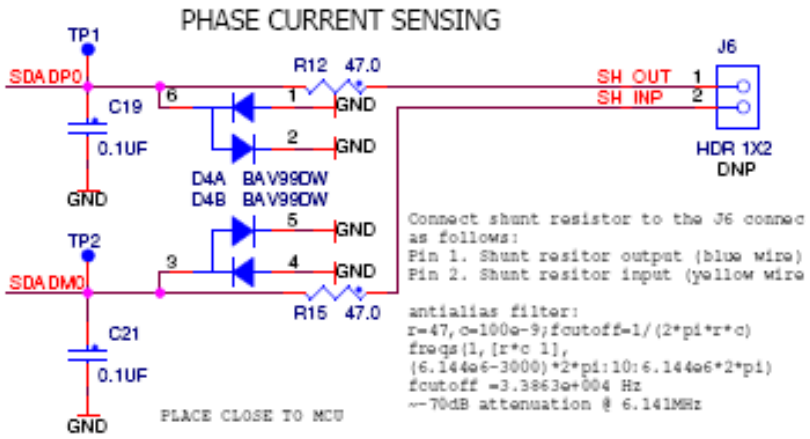
Sampling frequency and anti-alliasing

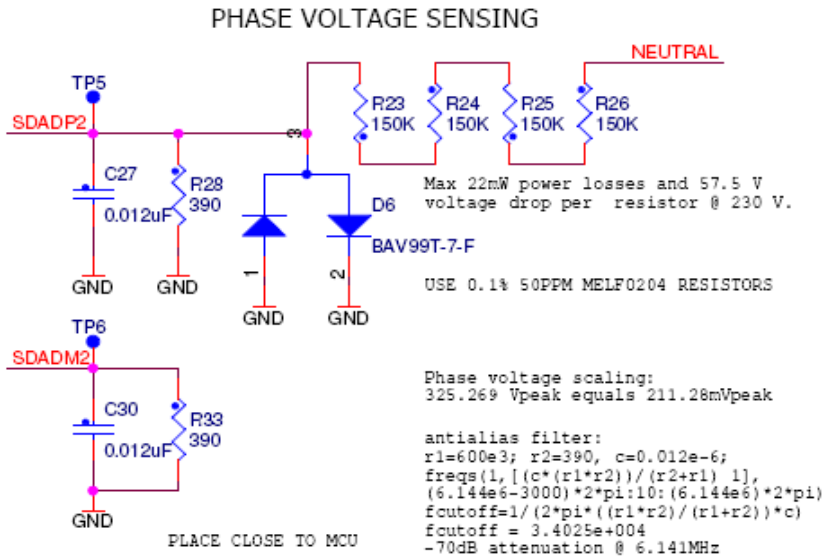
anti - aliasing filter used

- should not change phase and magnitude
- impedance should be 10-100 times smaller then ADC impedance
- voltage path has higher impedance to keep divider cross current low
- capacitor should be bigger then sample hold
- 51 Ohm -2uF, 1M-110pF, 1k-110nF



Sampling frequency and anti-alliasing signal tailoring and filters

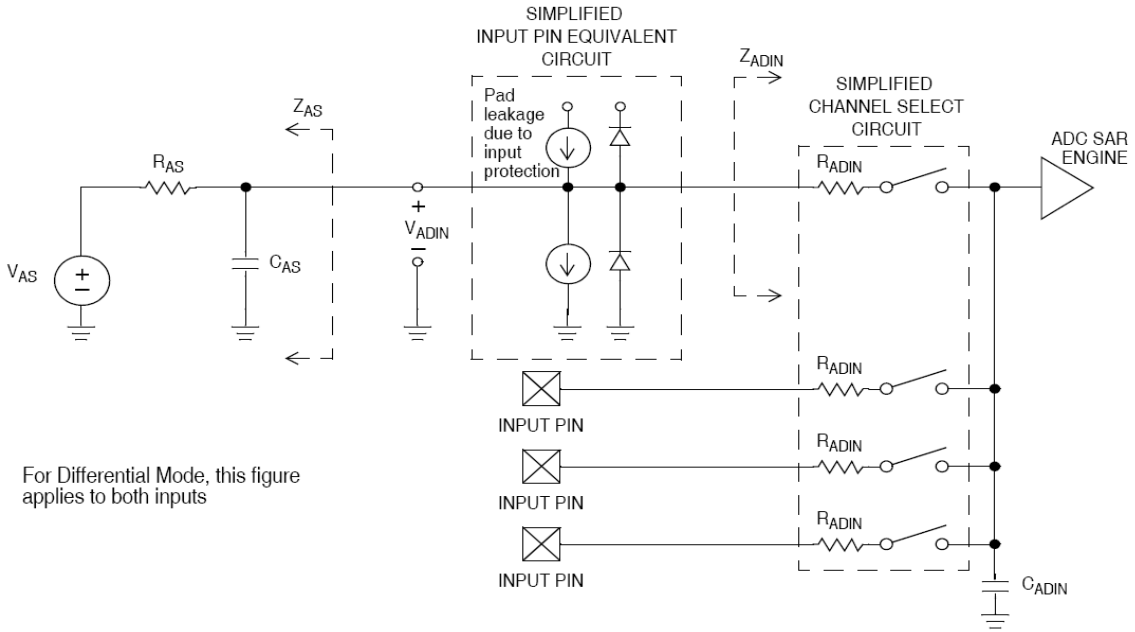




ADC additional parameters

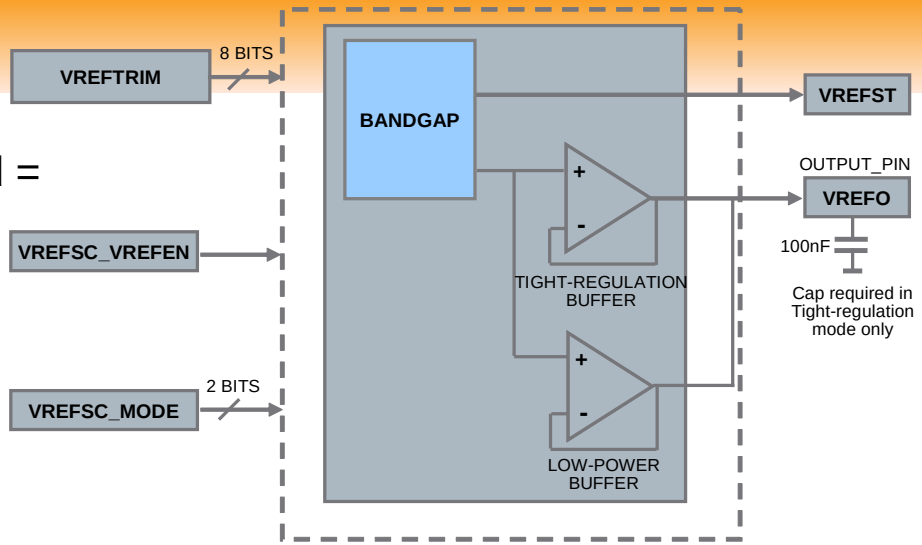
- synchronous – delayed start of converters for phase correction
- dynamic change of phase shift without interrupting sampling cycles
- In shunt mode need to
  use PGA 32x
- Single or differential mode
- +-250mVp input range
- high sensitivity
- gain error, offset error
  is not essential, calibration
- common mode rejection

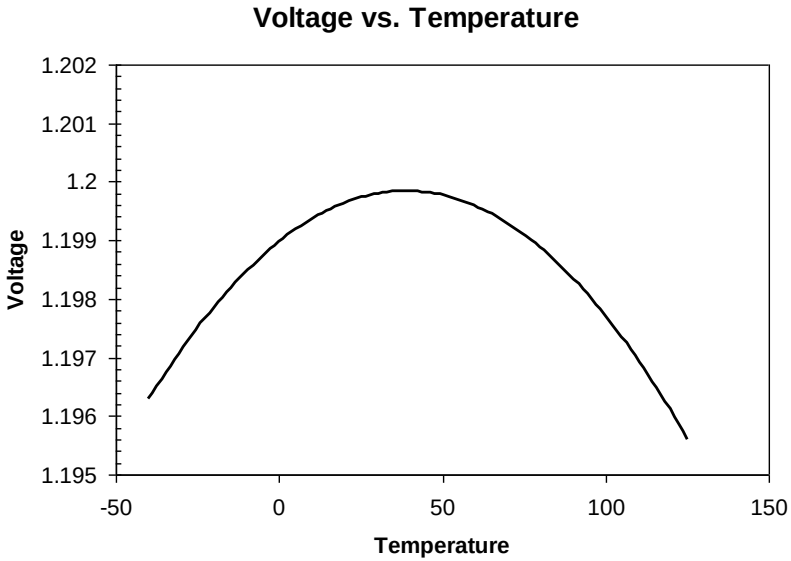
crosstalk rejection important



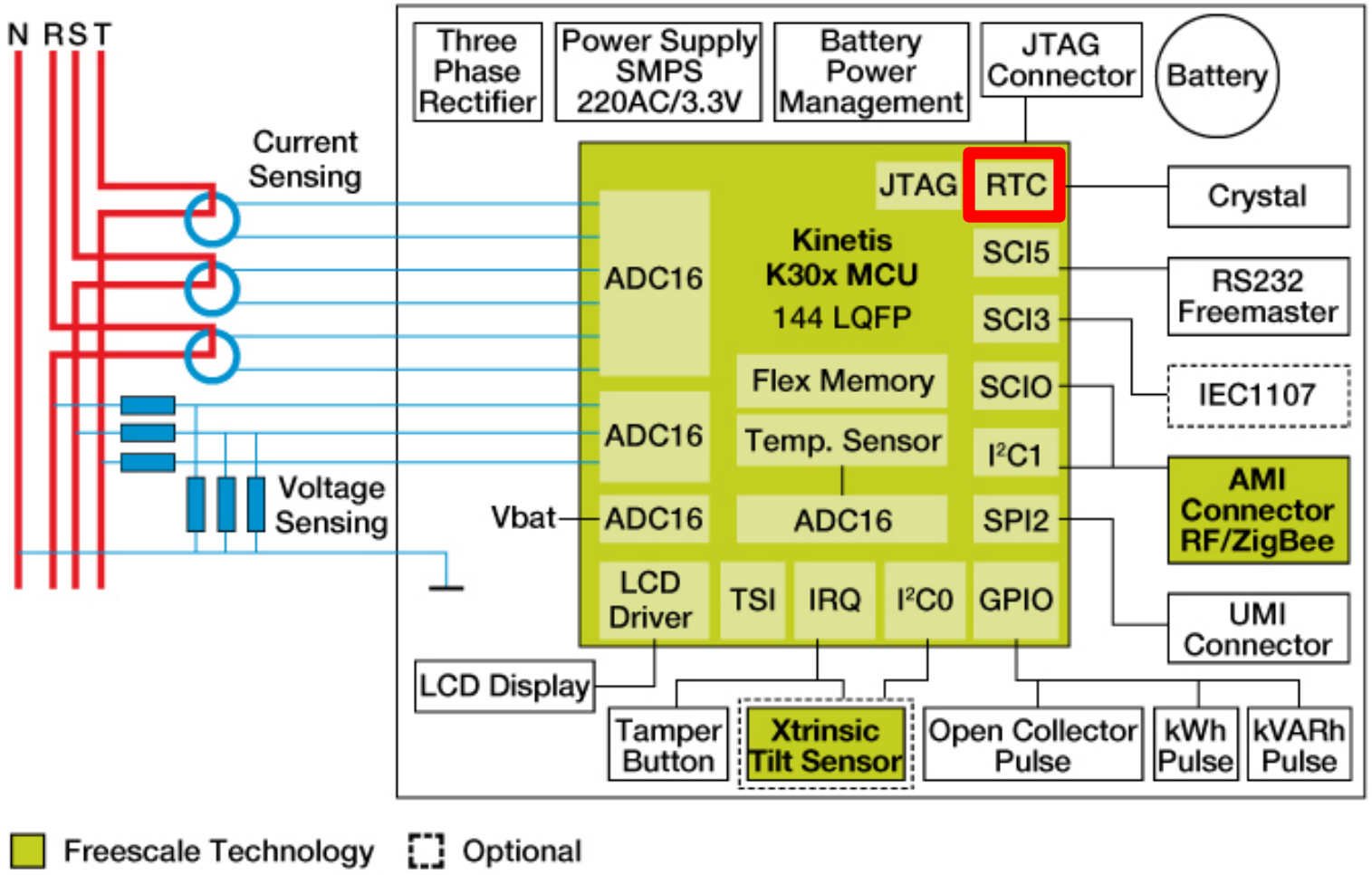
Voltage reference

- Bandgap diode serves as Votage reference Vd = 1.2V, compensated!
- 1.2 V output at room temperature, 30 ppm/C
  0.15% at 50 ° C
- EN 50470 add. error of 1,9% per 50° C
- Programmable trim register with 0.5mV steps, automatically loaded with factory trimmed value upon reset
- Dedicated output pin VREFO for external BIASING - up to 10mA load capability in tight-regulation mode
- PSR of 0±0.1 mV DC and -60dB AC



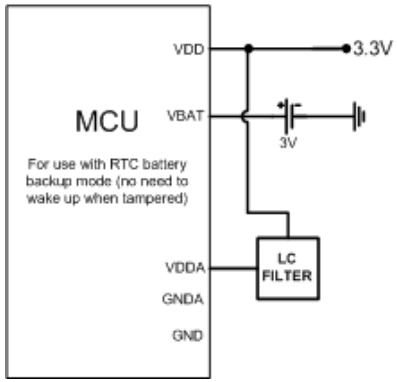


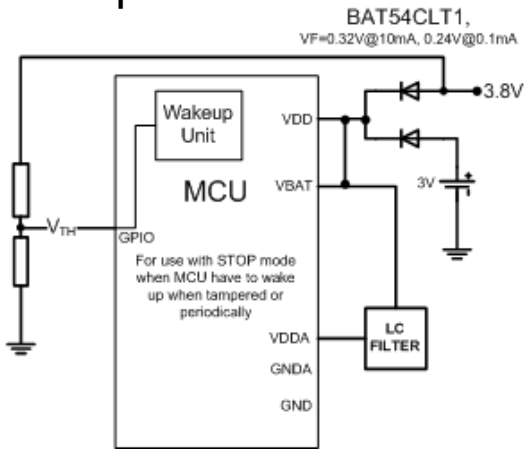
Single phase power meter block diagram

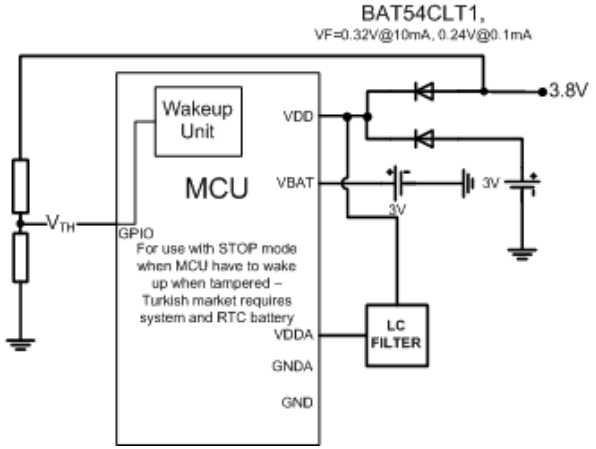


Real time oscillator and module

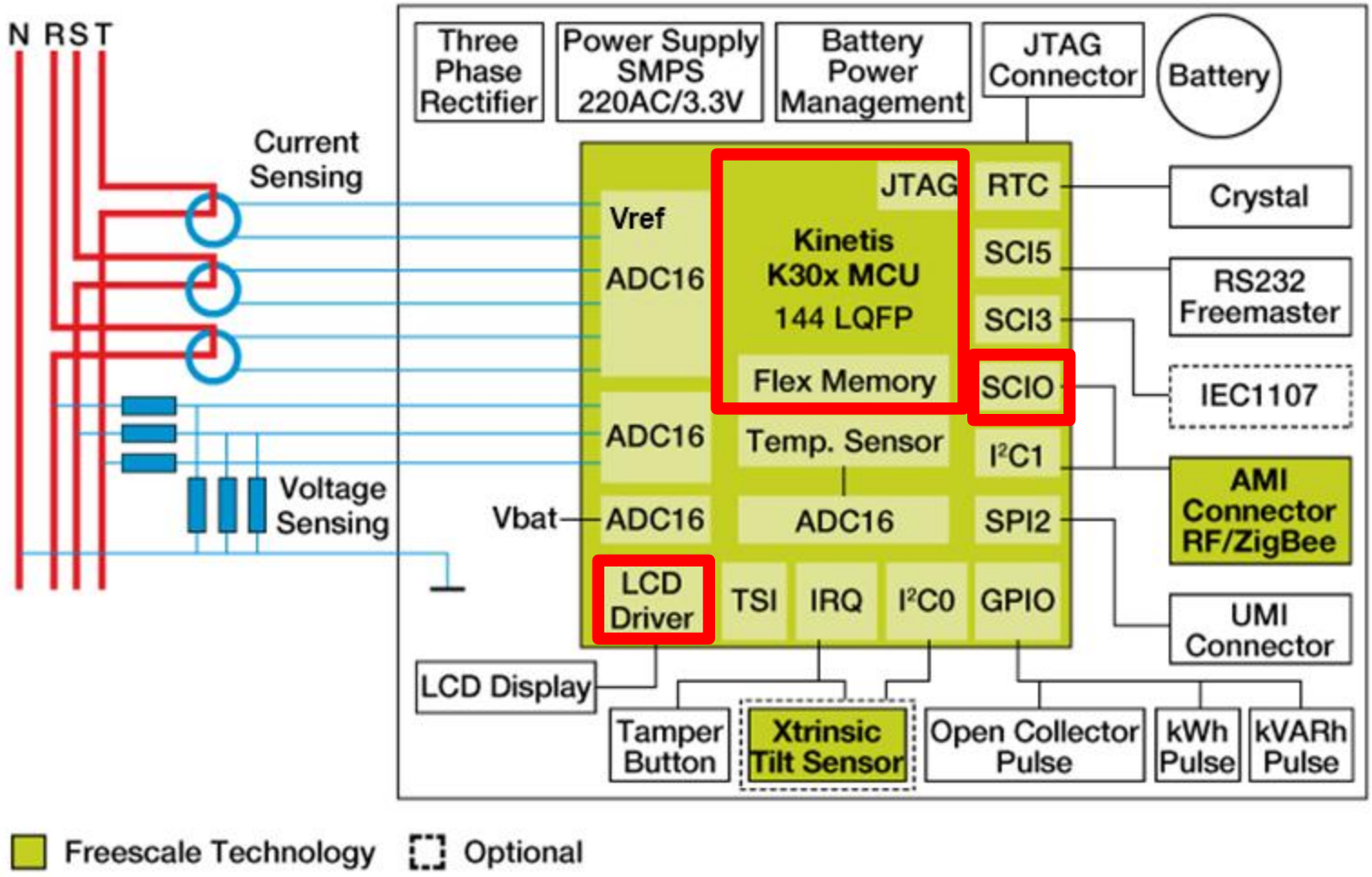
- Precise clock reference needed ~5ppm makes 2.6minuter / year error
- Real time clock must provide mechanism to calibrate either crystal by load caps or by digital
- Must work battery operated and provide 2 battery use case
- max 3.7V operational voltage for lithium batteries
- Alarm modes to wake up MCU when mains disconnected
- Tamper detection with tamper information written to EEPROM
- Up to 12 year of in the shelf live on
- Static versus dynamic tamper







Single phase power meter block diagram



Processor core performance

- for mentioned dynamic range 1:400 we need 32bit calculation
- for integrators or IIR filters 64bit -> 32 bit processor is more suitable
- 8 bit core is too slow, only single phase meter and active energy
- 32 bit processors are more suitable for meter design, ARM M0 single, M4 poly-phase
- calculation granularity can make a big difference in computational load
- Metering algorithms have small RAM, FLASH footprint
- DMA support with advantage

Table shows 8-bit calculation times @20MHz busclocks

19.92 MHz CPU @ 3200 samples/s	Cycles / multiplication	Cycles / sec @ 3200	CPU load [%]
16*16 -> 16 @ C lib	220	704000	~3.5
32*32 -> 32 @ C lib	620	1984000	~10
32*32->64 @ASM optimized	635	2032000	~10.2
32+32-> @ 32 C lib	229	732800	~3.6

Processor core performance

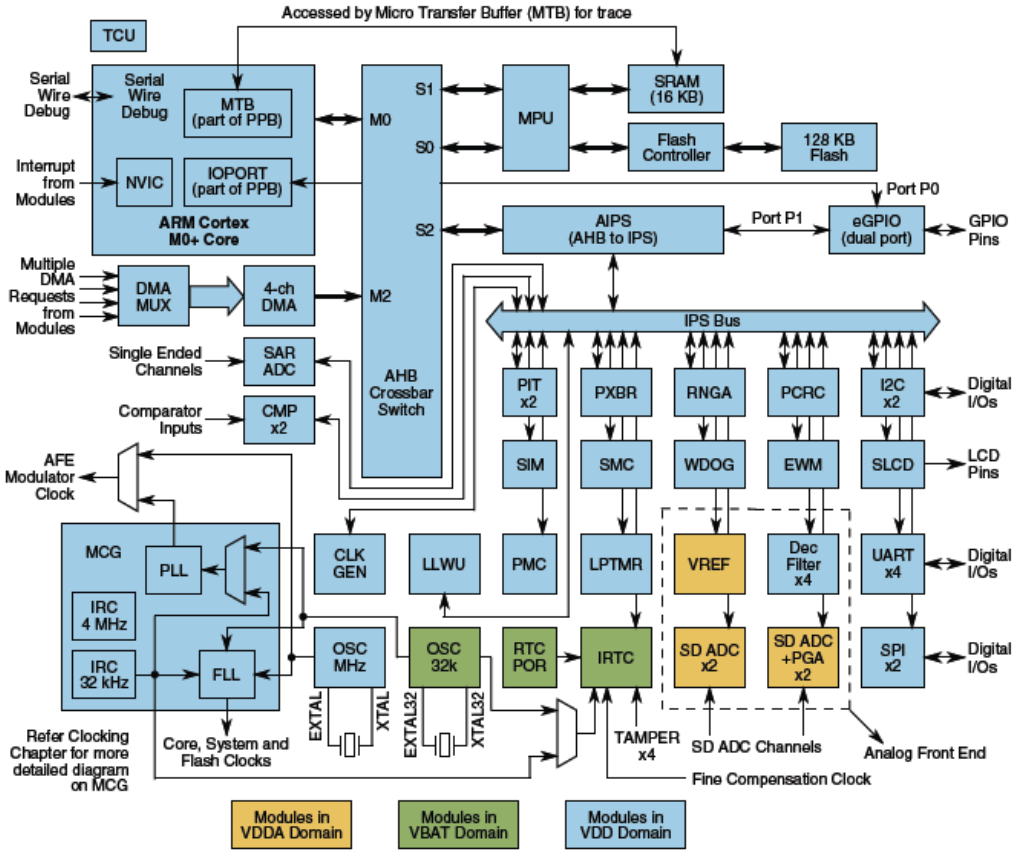
- Roughly number of cycles for calculation of Active and Reactive power (Hilbert filter) on ARM M0+ and M4 cores:

bus cycles	M0	M4
Active power	220	750
Reactive power	1000	2400

- Power consumption is essential in single phase power meter. Power consumption is tradeoff accuracy, chip size and skills, should not excess 5mA
- Power consumption in the sleep mode should be less then 1uA

Modern power meter MCU Freescale KM30

- LCD, frontplane, backplane
- comparator, filter , hysteretic
- DAC for threshold
- sleep modes + startup time and current
- in
- tampering detection ability
- EMI regarding tampering
- internal block connection
- VELMEC support



Existing MCU overview

- Smart Grid - general overview
- Power Meters
- accuracy requirements to actual power meters
- current, voltage sensors used in static meters
- single, two and three phase topologies
- energy calculation algorithms active and reactive energy
- microcontroller requirements ADC, DAC, tampers, RTC, CPU
- **existing MCU overview**

Metering processors on the market

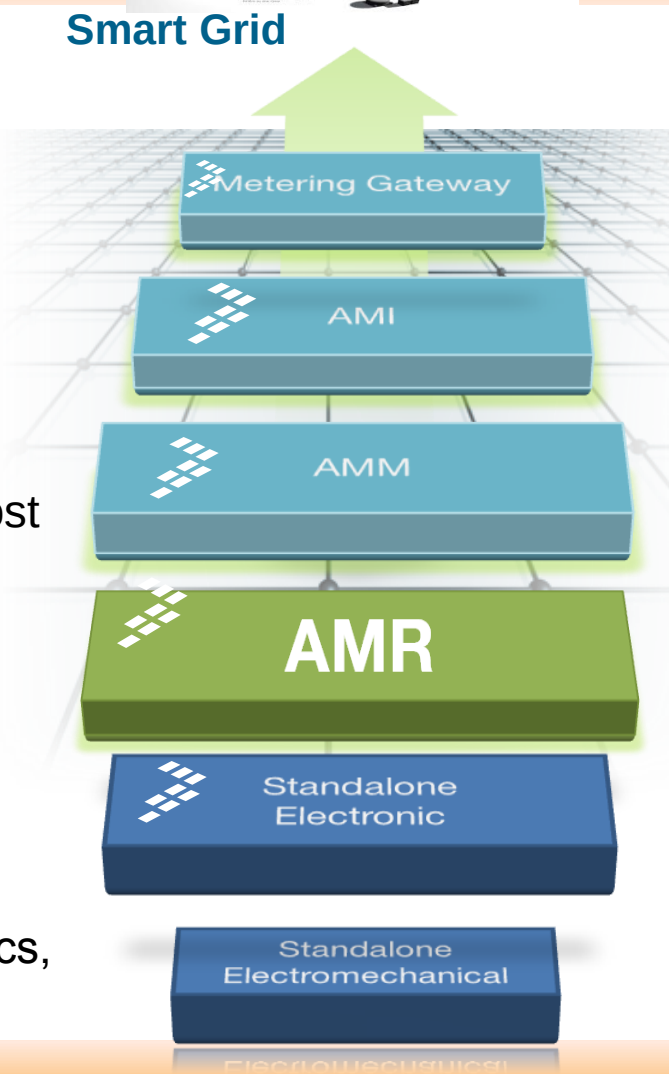
	Freescale KM3x	Texas Instr. MSP430F6736	Microchip PIC18F87J72	Renesas 78K0R/LG3-M
CPU Type/clock	32bit, 50MHz	16-bit, 25MHz	16-bit, 48MHz	16-bit, 20MHz
RAM/FLASH	16kB/128kB	4kB/128kB	3.9kB/128kB	7kB/128kB
RTC	YES	YES	YES	YES
Metrology engine	NO	NO	YES	YES
ADC type	SD24-bit, 94dB	SD24-bit, 87dB	SD24-bit, 90dB	SD24-bit,62dB
Input voltage range	+-250mV	+- 1V	+-6V,7kV HBM	+-0.375
Input impedance	200kOhm	200kOhm/PGA	350kOhm	na
PGA	1,2,4,8,16,32	2,4,8,16,32,64	2,4,8,16,32	2,16
Voltage reference	1.2V @	1.2V @18ppm	2.37V, 12ppm	1.2V

What smart grid is, grow drivers

- Smart Grid - general overview
- Smart grid
- **what smart grid is, grow drivers**
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- security short review

What makes Smart Grid Smart

Smart Grid will enable the power distribution network to support a bi-directional flow of power and communication capabilities from power distribution facilities to consumption locations



Functional applications for Smart Grid:

load control (shedding, scheduling, programming)
price awareness (immediate, advance notification, static, cost of use)
demand response (program participation, event opt in/out)
consumption awareness (whole-house, per appliance)
market messaging (promotions, message delivery)
remote access (consumer control via the internet)
installation & commissioning (discovery, registration, authorization)
user interface & network management (std GUI's, diagnostics, upgrades)

Smart Metering Market Enablers and Growth driver

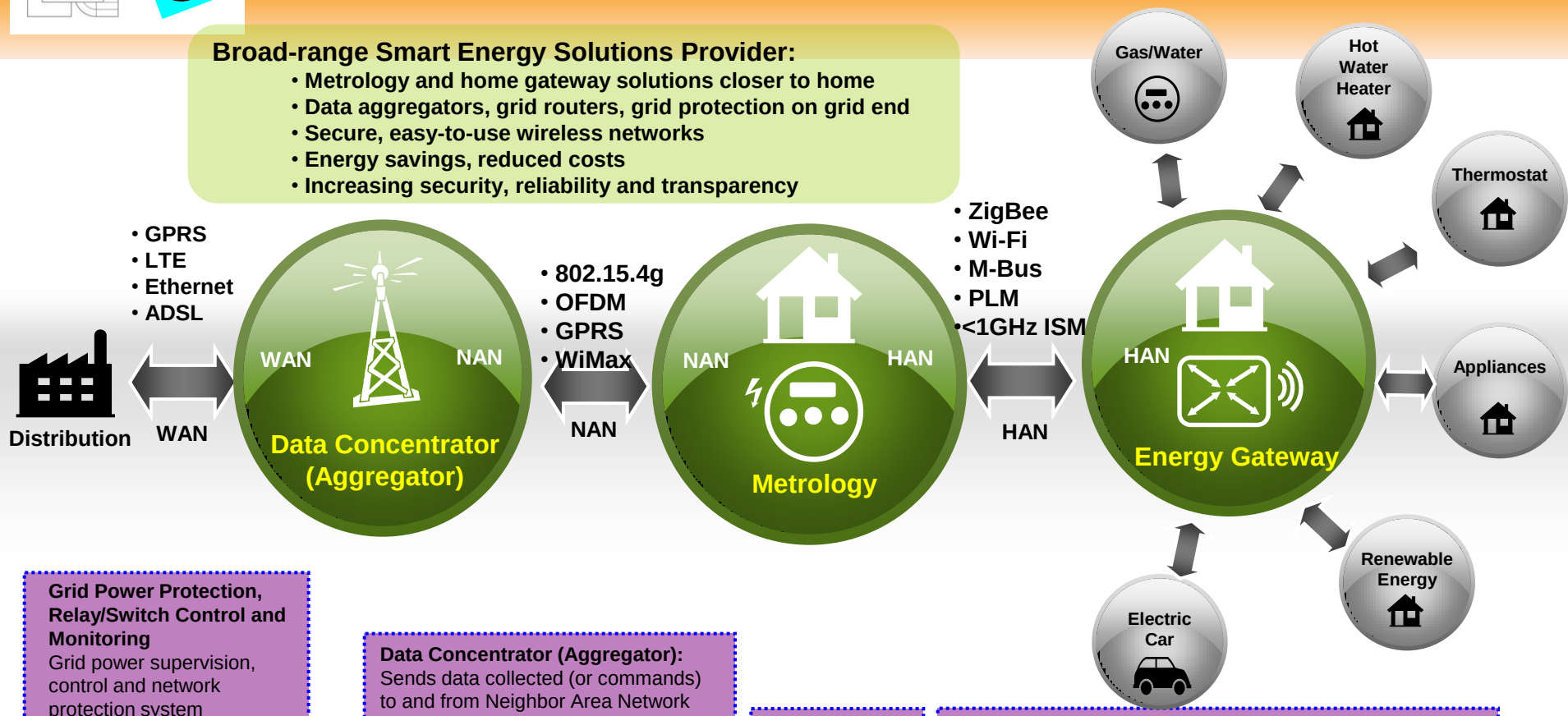
- Governmental Mandates
  - EU plans 20% reduction in energy consumption by 2020
  - Deregulation leading to separation of energy transport and energy provider
  - USA: $4.3 billion for direct investment in the smart grid through the stimulus package
  - China $9.7 billion investment to deploy AMR/AMI
- Utility Companies
  - Optimization of the distribution infrastructure and prevention of potential black-outs (peak management)
  - More services to end consumer
- Renewable Energies and E Vehicle
  - Residential solar and solar farm decentralized productions
  - Consumer production sold back to the energy provider
  - Plug-in hybrid electric vehicle (PHEV) cars

- In-Building Customer Comfort
  - e-thermostats, smart and user-friendly displays, home-automation
  - End-customer energy savings (controls when, how, how much)

Smart Energy network segments

Broad-range Smart Energy Solutions Provider:

- Metrology and home gateway solutions closer to home
- Data aggregators, grid routers, grid protection on grid end
- Secure, easy-to-use wireless networks
- Energy savings, reduced costs
- Increasing security, reliability and transparency



Grid Power Protection, Relay/Switch Control and Monitoring
Grid power supervision, control and network protection system solutions; protective relays and switches control for power grid

Data Concentrator (Aggregator):
Sends data collected (or commands) to and from Neighbor Area Network (NAN) or Home Area Network (HAN) to utility

Metrology:
Hardware that measures and controls flow of energy to/from building

HAN (Home Area Network):
Wireless or wired network used for load control and dynamic response by utilities
- Electric meter communicating with T-Stats, appliances, water heaters, pool pumps, electric hybrids, etc. (load control)
- Send pricing signals to consumers for smarter energy consumption (demand response)

Narrowband NAN Standards

Wireless

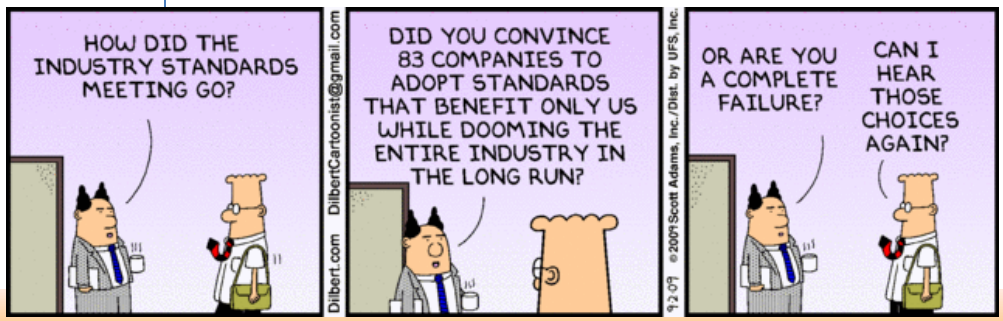
- Proprietary FSK solutions today
- Silver Spring Networks
- Sensus (FlexNet)
- Itron (OpenWay)

- IEEE 802.15.4g
- Strong participation by NAN industry players (L&G, Itron, Silver Spring, Sensus, etc.)
- FSK & OFDM modes

- Some companies using cellular
  - **GPRS**, **WiMax**, etc.

Standardized and proven PLC

- IEC 61334-5-2 **F**requency **S**hift **K**eyed
  - Capabilities and Characteristics
- IEC 61334-5-1 **S**pread **F**req **S**hift **K**eyed
  - **PLAN** Capabilities and Characteristics
  - Message forwarding principle
  - Technology maturity takes twenty years
- IEC 62056-8-3/NP **PLAN+**
- OFDM **PRIME**
  - Est. 2009, products available
- OFDM **G3**
  - Driven by ERDF but written by Maxi
  - Part of ITU G.hn PLC group of standards.



Smart grid elements, standards, regulations, freq. and data rates

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- **smart grid elements, standards, regulations, freq. and data rates**
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- security short review

What we expect from PLC

- Latency < 100mS
- Bandwidth > 32kbps
- Energy efficient (device < 0.5W, comm's < 0.3W, support standby modes)
- Plug & play (standardised profiles, trivial installation)
- Future proofing – firmware upgradeable
- Coverage > 95% of home AC wiring (~ 100m distance)
- Multi-phase – must cross split and three phase installations
- Multi-dwelling – up to 30 devices per logical network and 126 logical networks
- Compliance – support for transmit power control and a coexistence protocol
- Diagnostics – standardised link layer status/remediation
- Quality of service – Support for smart grid message prioritization
- Security – logical link separation per physical channel, encryption to CSWG

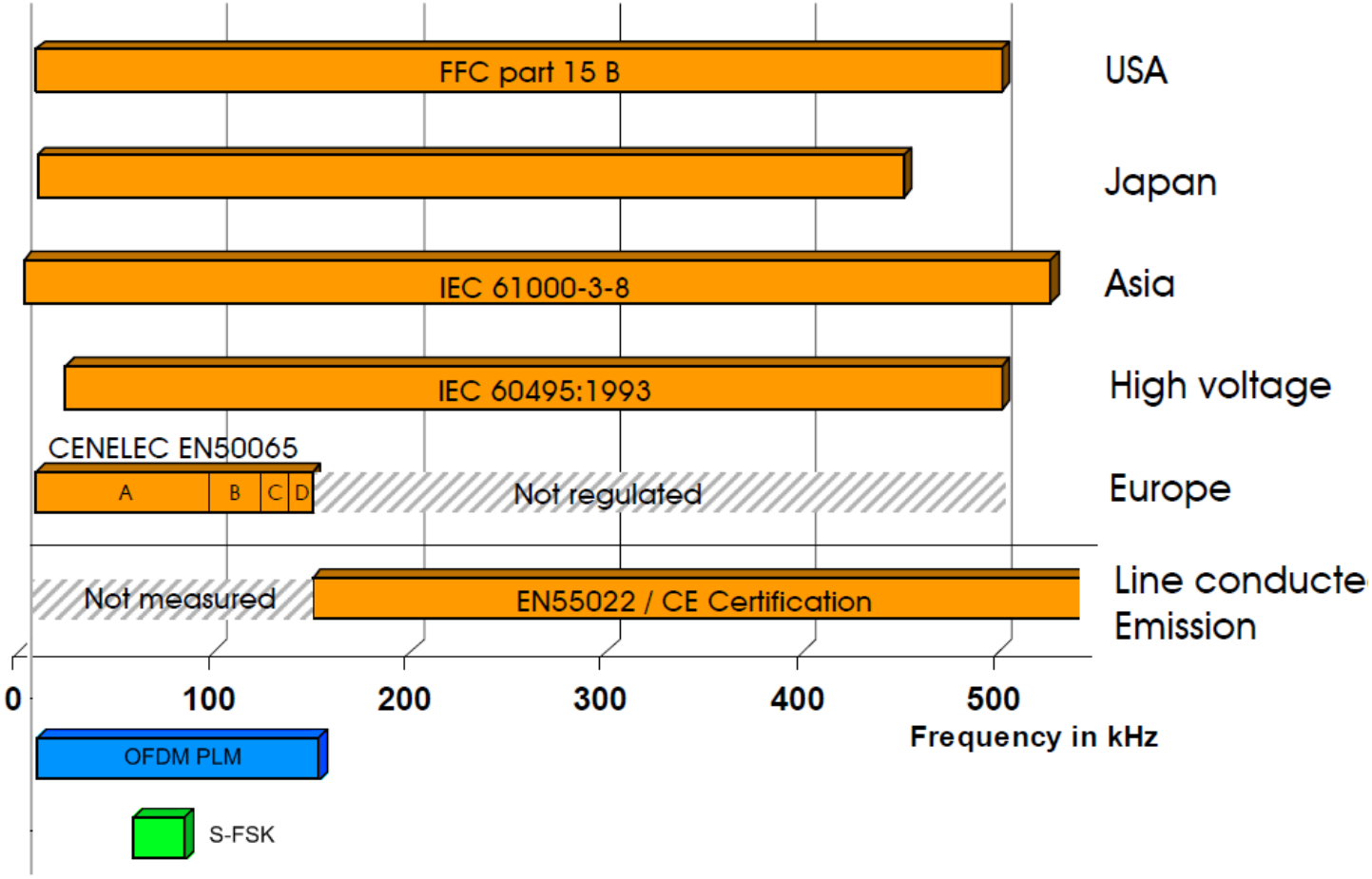
Power Line Communication

	Low Data Rate	High Data Rate	Broadband
Data Rate	< 10kbps	50kbps <..< 1Mbps	> 5Mbps
Frequency Range	9-150 kHz	9-500 kHz	1.5-50 MHz
Load/Noise/Attenuation	low impedance / big noise / long distance	middle impedance / middle noise / middle distance	high impedance / low noise / short distance
Modulation	single/dual tone FSK, BPSK, S-FSK	multicarrier OFDM	multicarrier MCM / COFDM
CPU	DSP < 50 Mips	> 100Mips,	Specialized hw. accelerators, ASIC
Application	AMR, Home Control	Smart Grid, Airfield Lighting, Advanced Meter Management	Last Mile Telecom, Internet, VoIP, HDTV, AV
Existing standards	ST, Echelon, YITRAN, Maxim	iAd, Maxim, Ti, Echelon	DS2, Intellon, arKados

OFDM evolution – PRIME, G3-PLC

Parameter	PRIME	G3	FlexOFDM
Modulation Size	DBPSK / DQPSK/D8PSK	DBPSK / DQPSK/(D8PSK)	DBPSK/DQPSK/D8PSK/ Coherence Modulation
Forward Error Correction	Rate ½ Convolutional Code	Outer RS + inner rate ½ convolutional code	Outer RS + inner rate ½ convolutional code
Data Rate (Cenelec-A)	21, 42, 64, 84, 64Kbps (PHY rate w/ coding)	20.36,/34.76/(46) Kbps (with coding)	Scalable up to 128Kbps
Band plan	Continuous 42-89 KHz (defined for LV scenario)	36-91 KHz with tone masking for SFSK	Variable: 3KHz in sub-A band, 12KHz in FCC, 24KHz in A, B, C band Wider sub-band in FCC
ROBO Mode	No	Yes	Yes
Link adaptation	Data only	Data + limited band plan	Data + more band plan
Interleaver	Only 1 symbol over frequency (2 msec)	time and frequency interleaving (Up to 175 msec)	>8ms (PRIME+G3 variation)
MAC	PRIME proprietary	802.15.4	PRIME, 802.15.4, IEC64334, other
Convergence Layer	IEC61334-4-32/IPv4	6LoWPAN/IPv6	any
Application	COSEM/DLMS, IP	COSEM/DLMS, IP	COSEM/DLMS, IP

S-FSK, OFDM data rate and band



CENELEC specifications

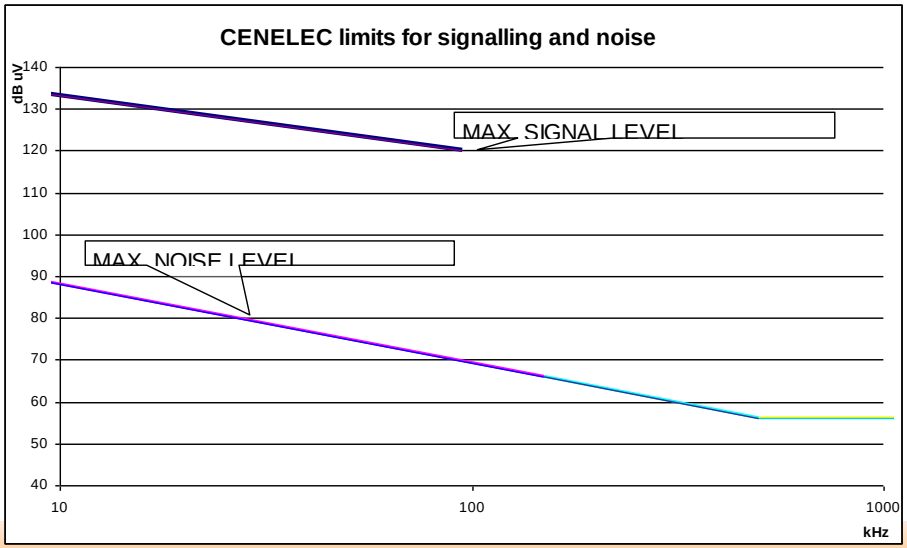
- **Cenelec bands :**
  - A 9-95kHz reserved for utility providers (out of house)
  - B 95-125kHz consumer no protocol (in house)
  - C 125-140kHz consumer access protocol (in house)
  - D 145-148.5kHz consumer (in house)

CENELEC specifies signaling and radiation limits and it's measurement

Signaling limits	**Single phase**	**3-PH, single ph. sig**	
Freq. ranges		**All ph. signal.**	**Single ph. Signal**
3kHz to 9kHz	134 dBuV	128 to 114 dBuV	134 to 120 dBuV
9kHz to 95kHz narr. band	134 to 120 dBuV	128 dBuV	134 dBuV
9kHz to 95kHz wide band	122 dBuV	116 dBuV	122 dBuV
95kHz to 148,5kHz	134 dBuV	128 dBuV	134 dBuV

CENELEC specifications

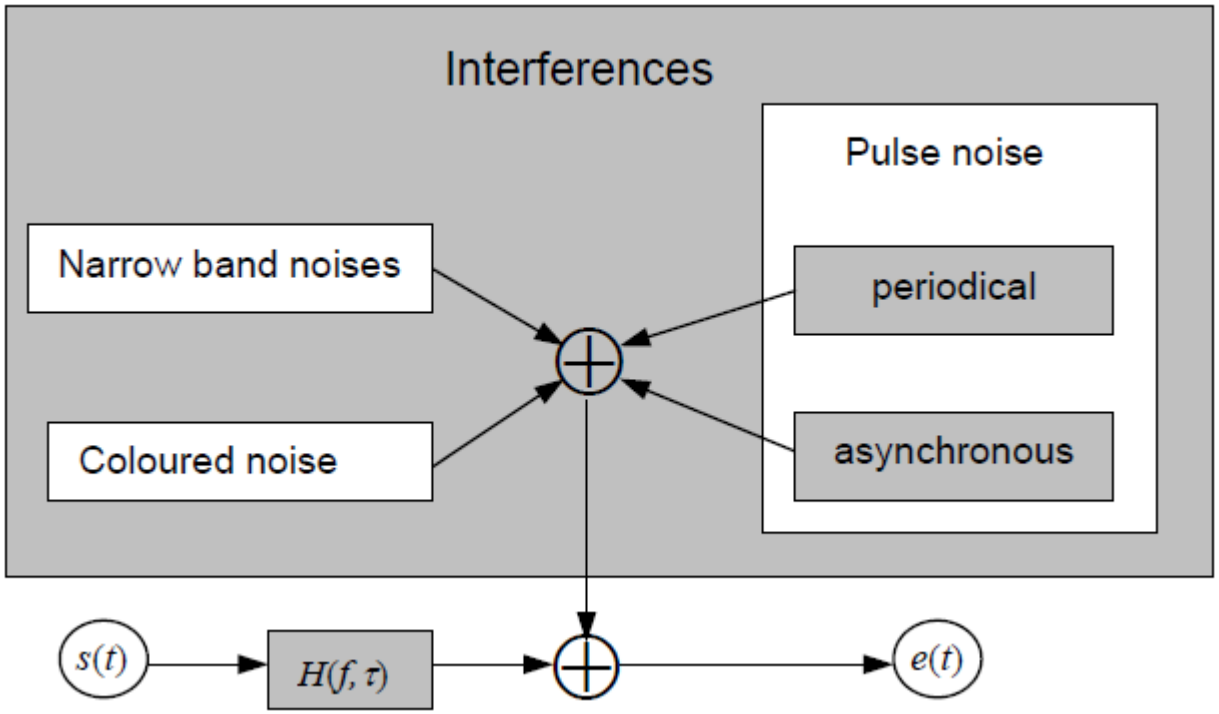
Disturbance limits	Limits [dBuV]	
Freq. ranges	**Quasi peak**	**Average**
3kHz to 9kHz	89dBuV	
9kHz to 150kHz	89 to 66 dBuV	
150kHz to 500kHz	66 to 56 dBuV	56 to 46 dBuV
500kHz to 5MHz	56 dBuV	46 dBuV
5MHz to 30MHz	60 dBuV	50 dBuV



Power line transmission channel definition

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- **power line transmission channel definition**
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- security short review

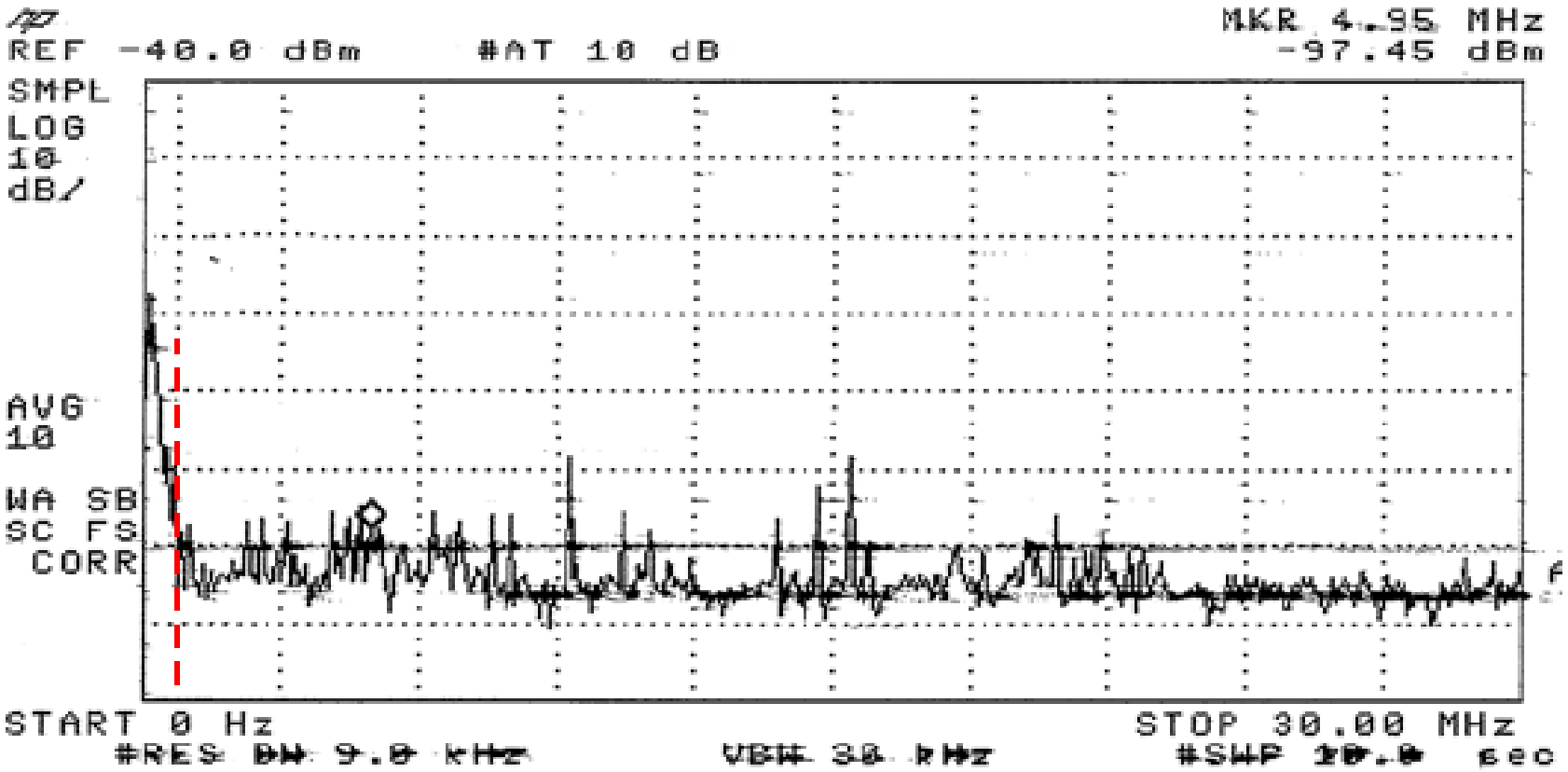
Transmission channel transfer function & noise



Mains represents really **hostile environment**!

PLC requires special techniques to overcome it

Transmission channel noise

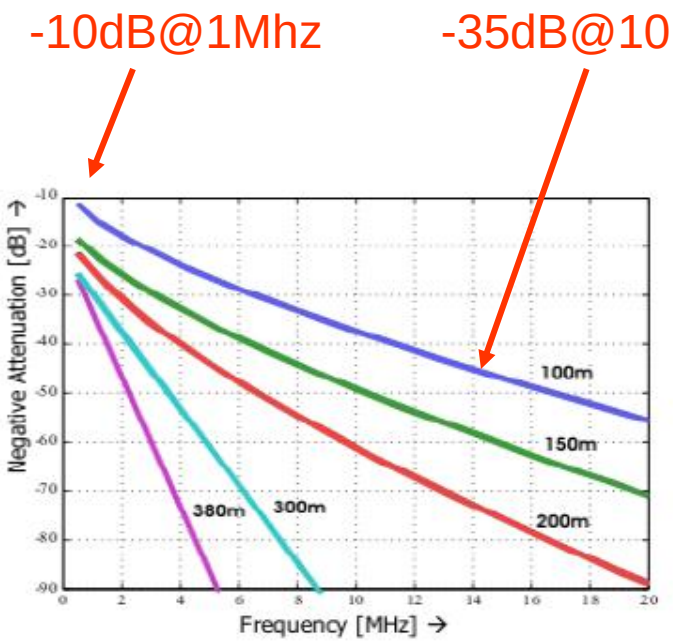


frequencies **bellow**

500kHz are very **noisy**

whilst **lower** background noise for freq **> 1MHz**

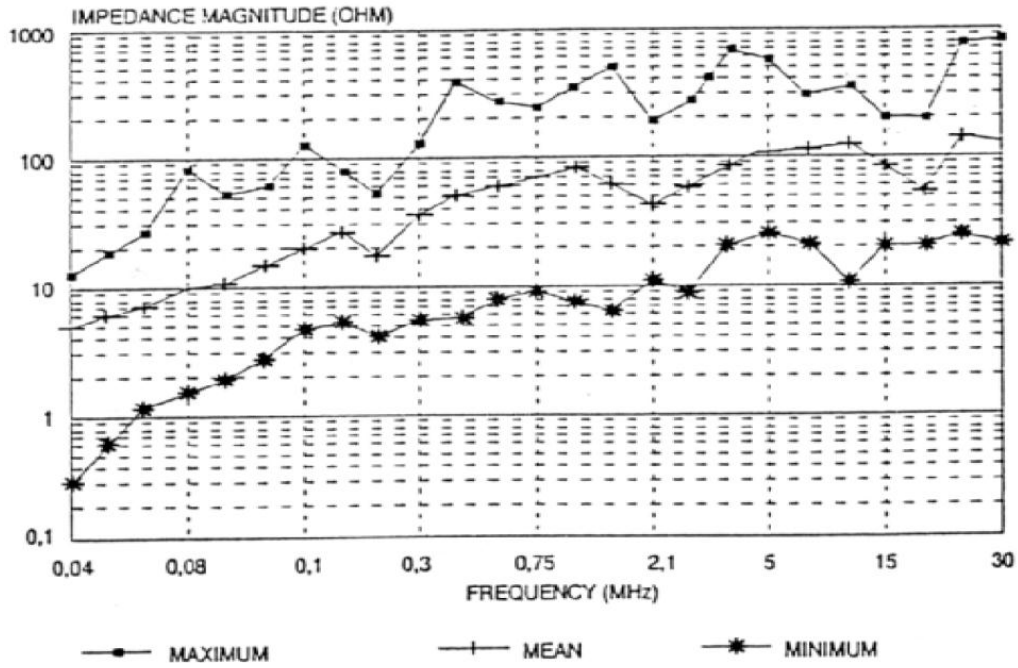
Transmission channel



attenuation for different cable length and frequencies

- **higher frequency** suffer from **higher attenuation** on the cable
- **low/middle speed** modems might reach **longer distances**
- receiver should overcome ~80dB dynamic range

Power Line – Coupling Impedance



- impedance **under 1Ω** for frequencies <150kHz
- higher impedance for higher frequencies
- dynamic impedance in long/short time period

In band noise with PLC systems

noise on receiver

transmitted signal

strong narrow band noise is **critical for single carrier modulation**!

Even multiple carriers may be affected due to receiver saturation

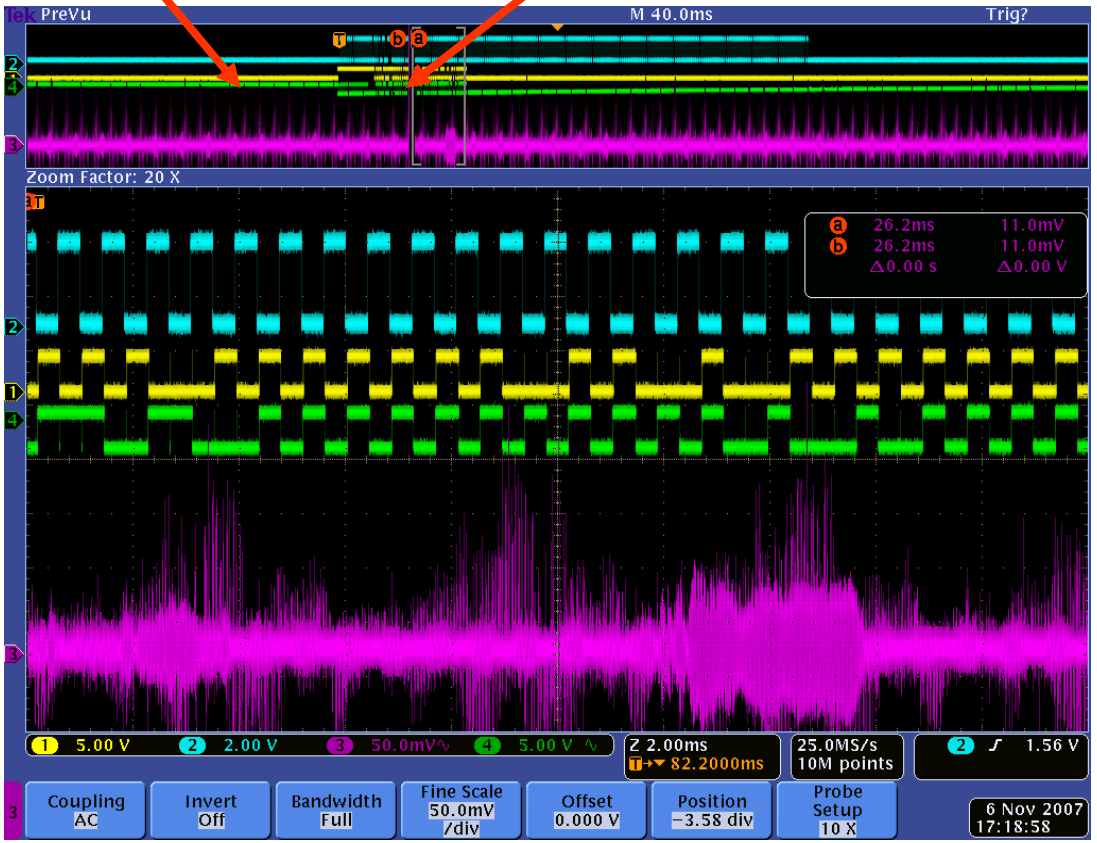
Receiver dynamic range is essential

Impulsive noise how to handle it?

impulsive noise synchronous

impulsive noise asynchronous

- switching mode power supplies, motor drivers,
  HVAC
- advanced methods like **FEC, interleaving, scrambling**
  is essential
- channel fading due to dynamic load

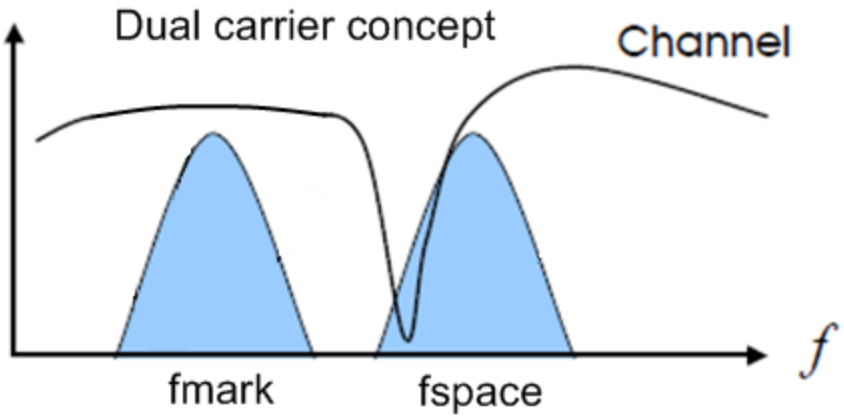


S-FSK modulation details PLAN

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- **S-FSK modulation details PLAN**
- OFDM modulation details and G3 protocol details
- Analog Front End details
- security short review

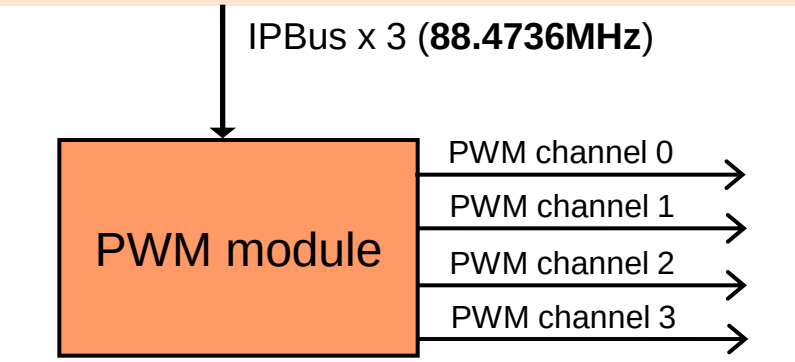
FSK modulation & PLAN

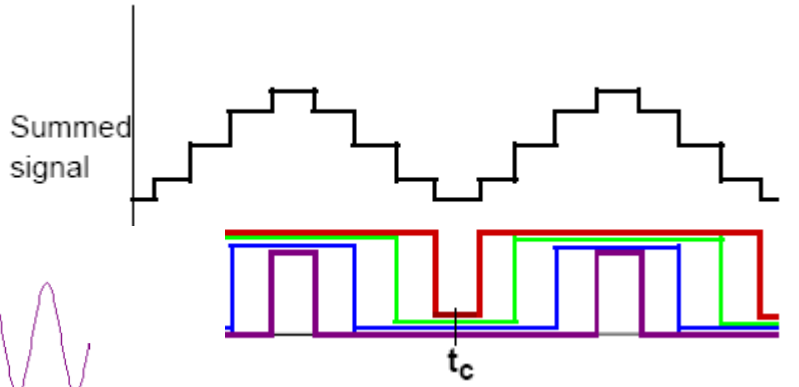
- Two frequencies that are fairly well separated > 10kHz
- At least one should be out of noise
- The receiver looking for FSK modulation on both channels.
- The Data Concentrator is the master on the PLC network.
- No slave (PLC device) can talk without receiving a request from the Data Concentrator.
- New generation S-FSK (PLAN+) does allow spontaneous transmission of alarms from the meter.
- There can't be collisions
  at a repeater level
- PLC device cannot initiate a communication with the Data Concentrator if necessary
- simple modulation easy to implement
- Freq. hopping tech. no available
- conventional DSP for decoding

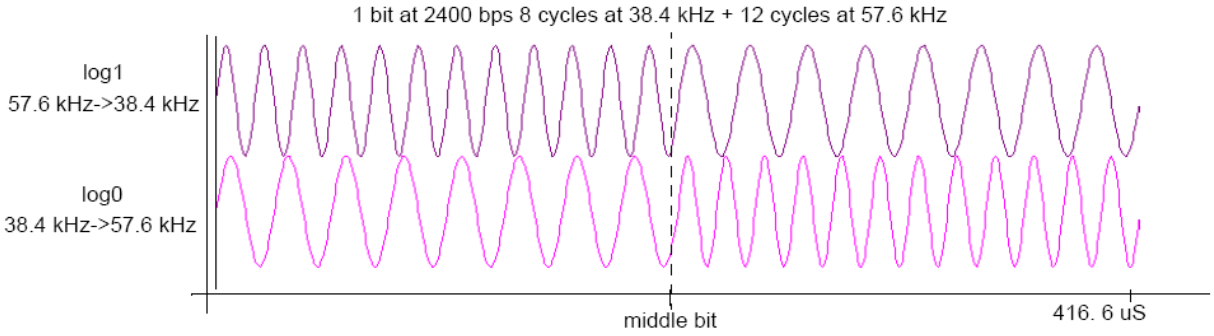


S-FSK Transmitter

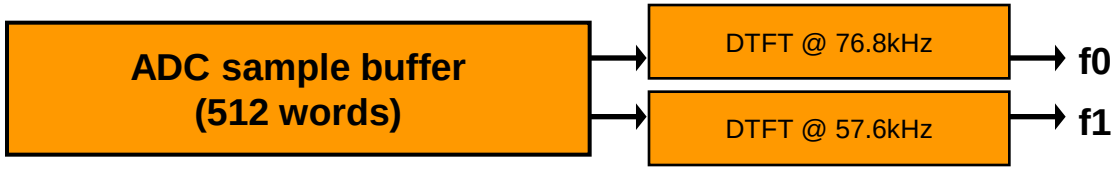
- two communication channels with delta frequencies > 10 kHz
- enhanced communication robustness in a hard noisy environment
- manchester coding may be used to handle dynamic loads (not PLAN)
- thought DAC requirements! 300ksmp/s
- center aligned PWM may be used





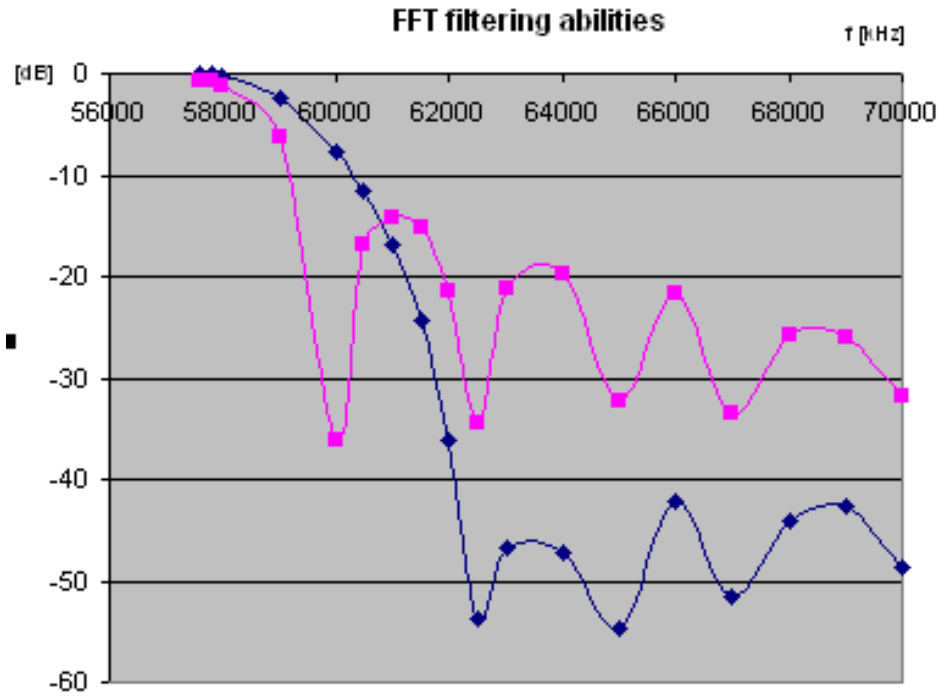


S-FSK Demodulation



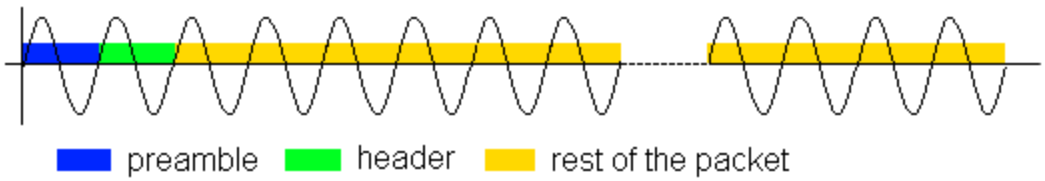
signal “energy” levels at the discrete frequencies

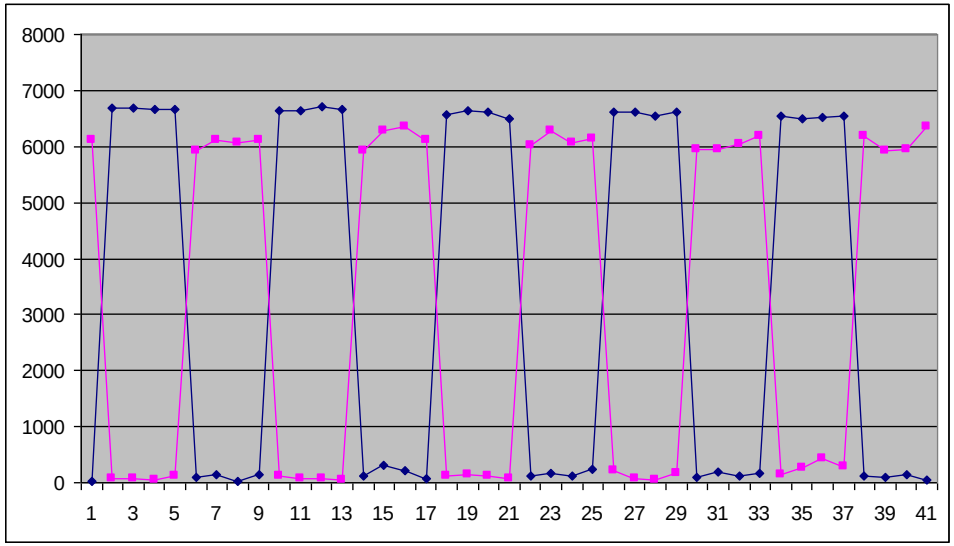
- due to coupling, impedance S-FSK signal goes to ASK frequently
- hard to mix. In digital
- precise PLL is costly – 2 freq. needed
- mark – space filtering method
- decoded using discrete Fourier Transformation
- frequencies chosen to have lowest possible interferer (filter transfer function)
- 1.2MHz sampling rate to get sharp filter response
- tough ADC requirements 70dB



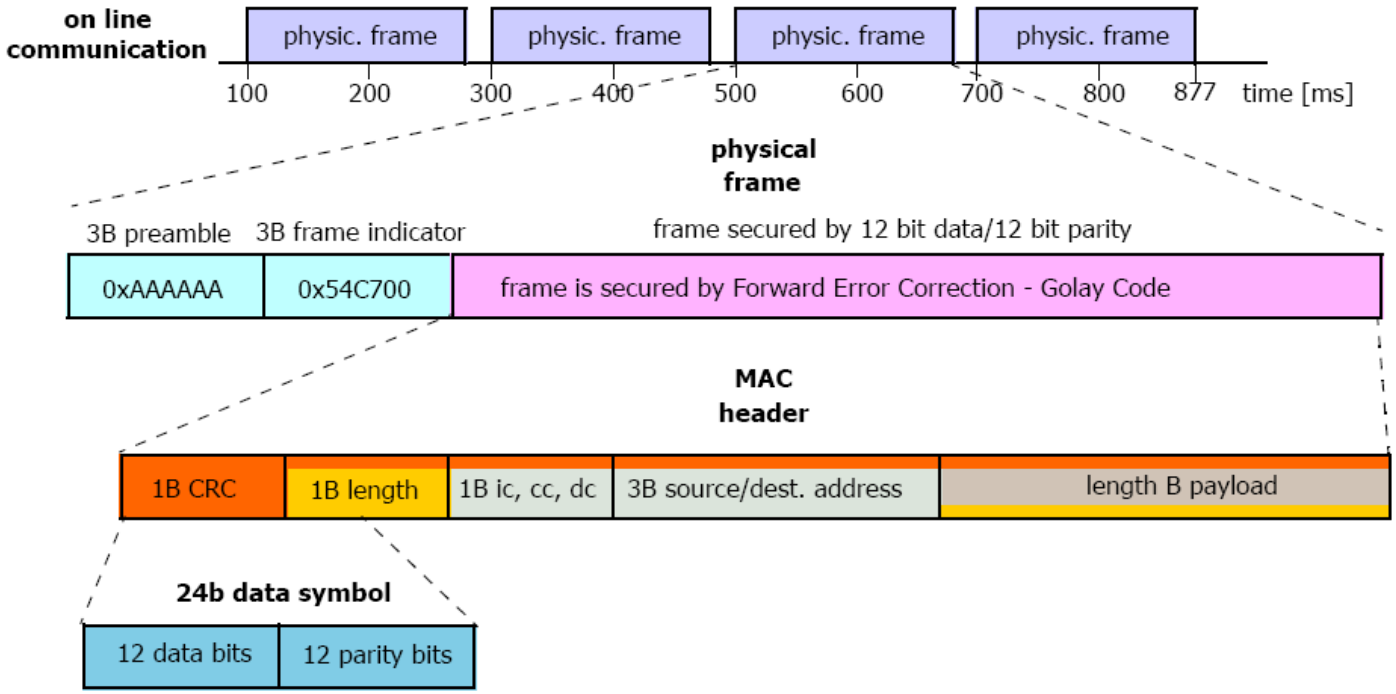
S-FSK packet wise, bitwise synchronization

- modem is fully mains **zero cross** (50/60Hz) **synchronized**
- bitwise synchronization done by preamble detection and bit synchronization technique 0xAAAA
- packet identified by header recognition 0x54C7

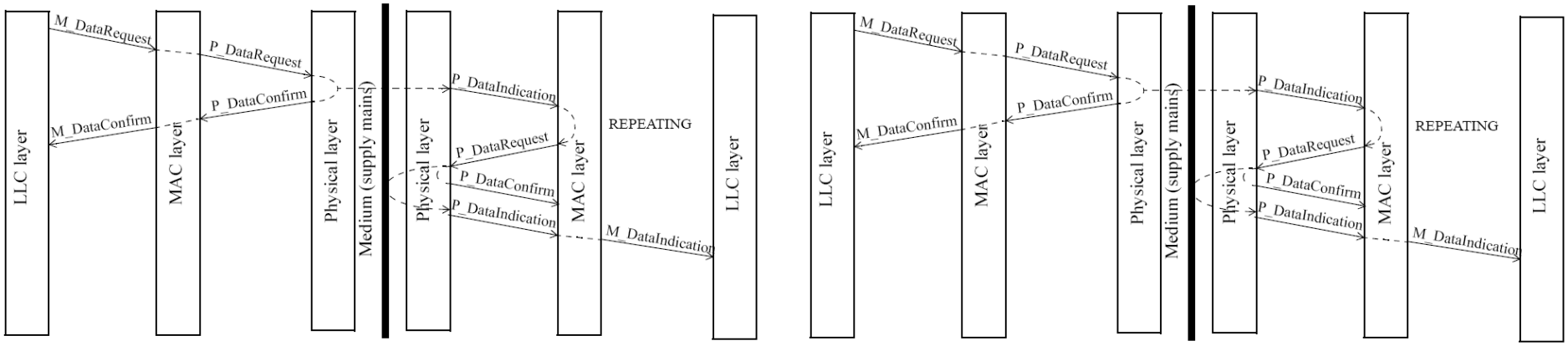




S-FSK packet structure



S-FSK REPEATING TECHNIQUE

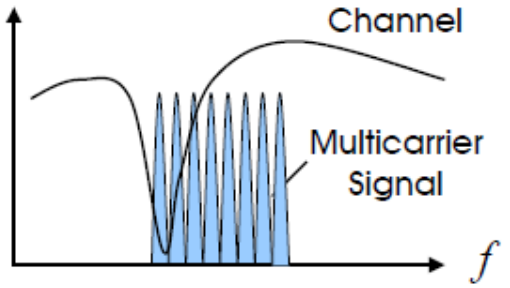


OFDM modulation details and G3 protocol details

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- **OFDM modulation details and G3 protocol details**
- Analog Front End details
- security short review

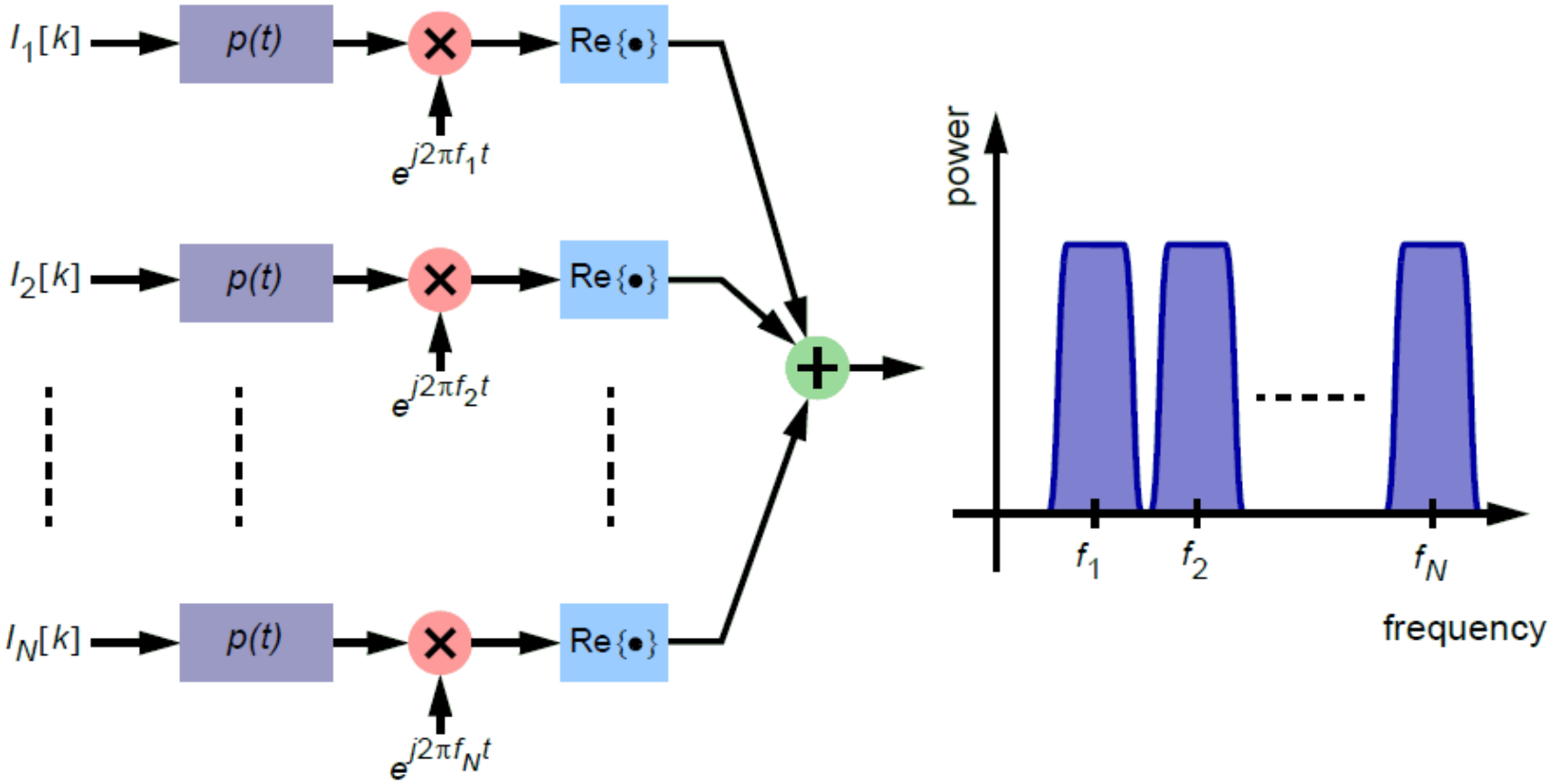
Multi carrier modulation OFDM

- **O**rthogonal **F**requency **D**ivision **M**ultiplex is multi-carrier modulation
- channel divided into narrowband flat fading subchannels
- OFDM is more resistant to frequency selective fading than single carrier
- channel coding and interleaving one can recover symbols lost due to the frequency selectivity of the channel.
- channel equalization becomes simpler than single carrier systems
- flexible resource allocation depending on channel characterization
- It is possible to use maximum likelihood decoding
- less sensitive to sample timing offsets than single carrier systems
- good protection against cochannel interference and impulsive parasitic noise
- the OFDM signal has a noise like amplitude with a very large dynamic range with high peak to average ratio
- sensitive to carrier frequency offset and drift



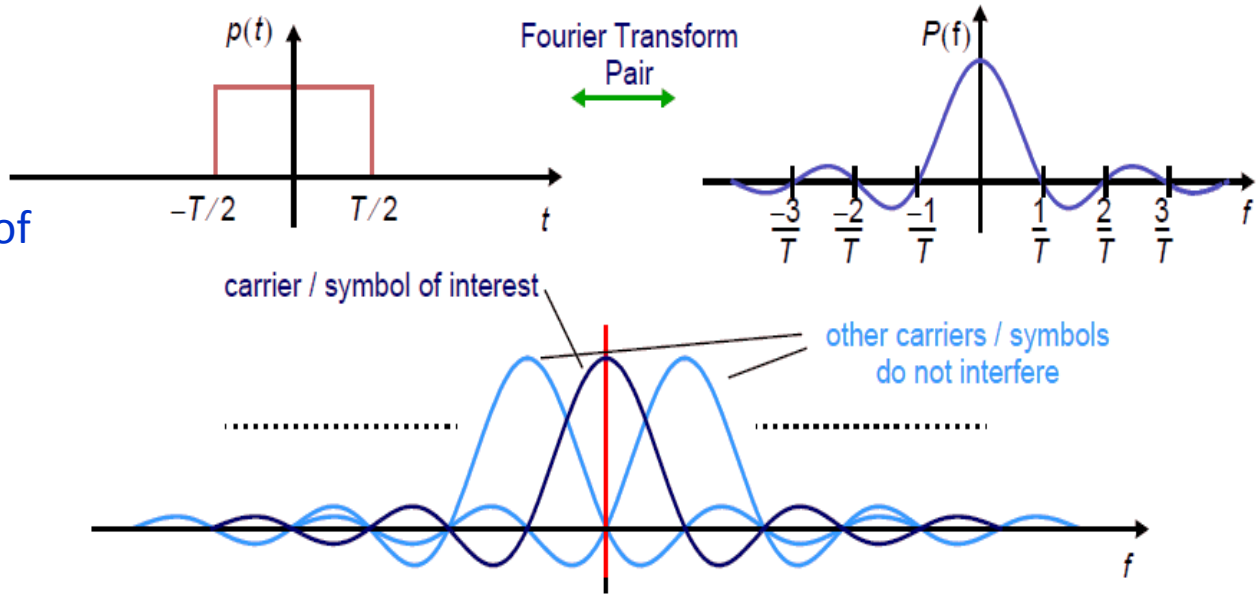
Multi carrier modulation OFDM

- OFDM is computationally efficient by using FFT and IFFT



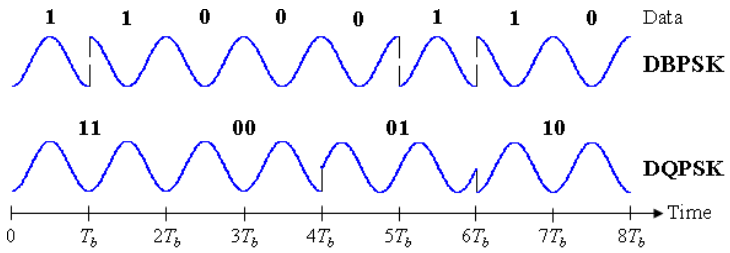
MULTI

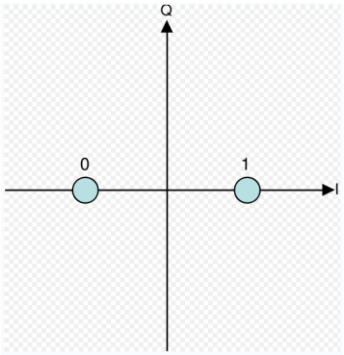
- zero inter-symbol interference due to cosine pulse shape with
- zero crossing at multiples of subcarrier

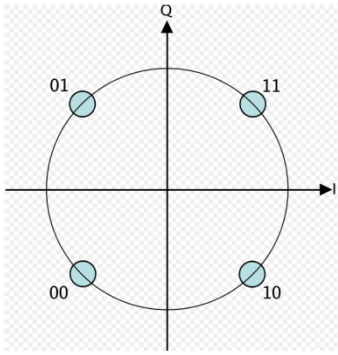


subcarriers may use different modulation schemes BPSK, QPSK

Channel definitions, modulation scheme is intention of standards PRIME, G3

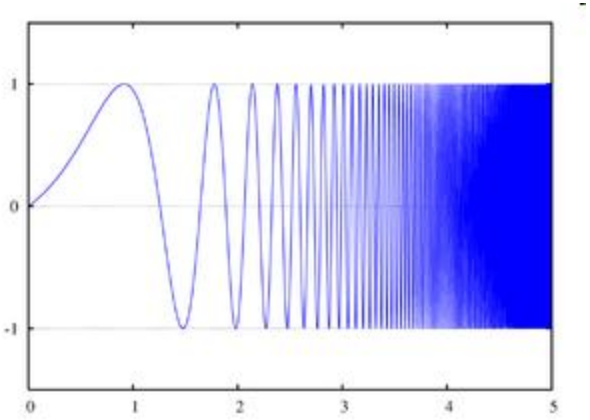




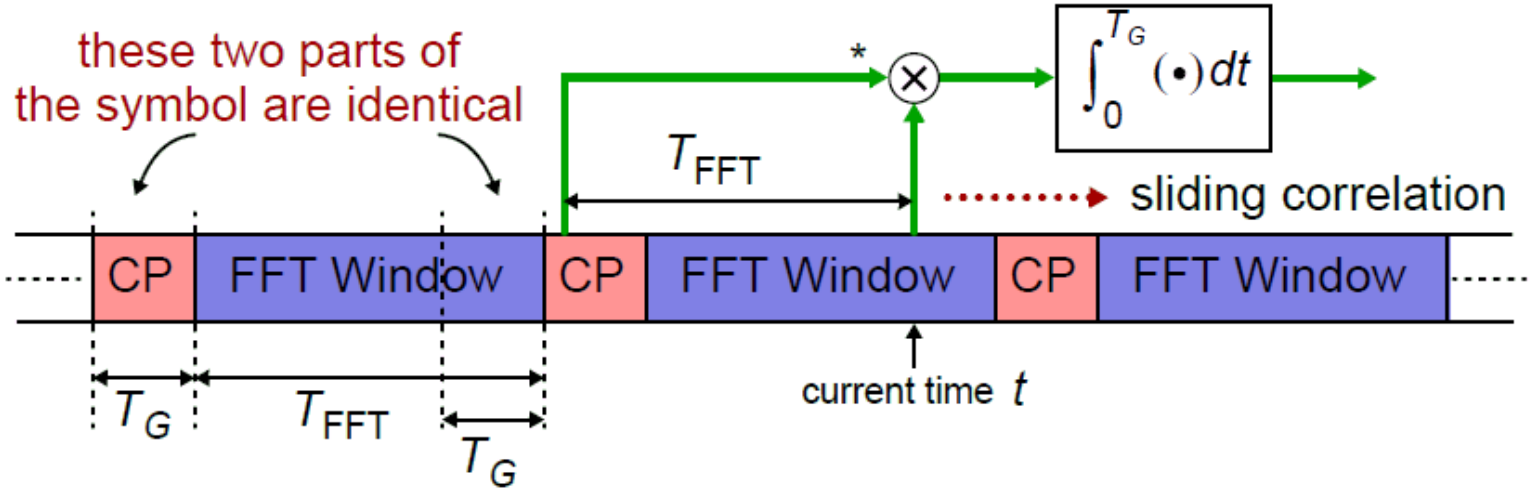


OFDM SYMBOL WISE, PACKET WISE SYNCHRONIZATION

packet synchronized using "**chirp**" signal
excellent autocorrelation capabilities
huge amount of energy
requires high computational power



symbol-wise synchronization by "**cyclic prefix**"

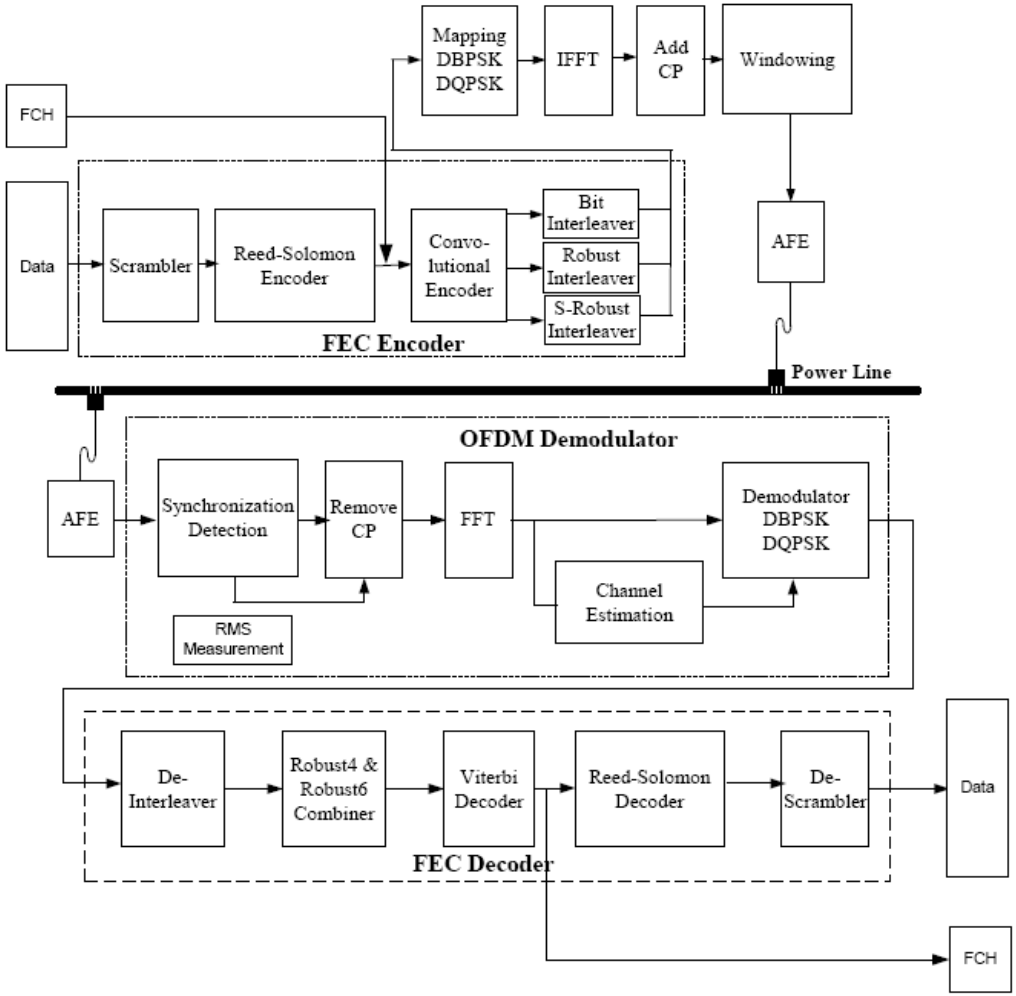


PLC 3G PHYSICAL LAYER DEFINITION

- PLC G3 uses 35.9kHz to 90.6kHz of the CELENEC-A band
- normal mode - OFDM with DBPSK and DQPSK per carrier
- robust mode adds 4 repetitive code
- phases of carriers in the adjacent symbol are taken as reference for detecting the phases of the carriers
- sampling frequency for receiver / transmitter is 400kHz
- considering 20ppm crystal accuracy the number of carriers is set to 36
- frequency range 35.938 to 90.625
- frequency notch for PRIME interoperability 63.3kHz-73.8kHz
- various modulation scheme and convolution coding is chose for given packed and required communication speed and robustness

3G is ERDF with Maxim IC driven standard and following pages points to it

PLC 3G PHYSICAL LAYER DEFINITION - SYMBOL

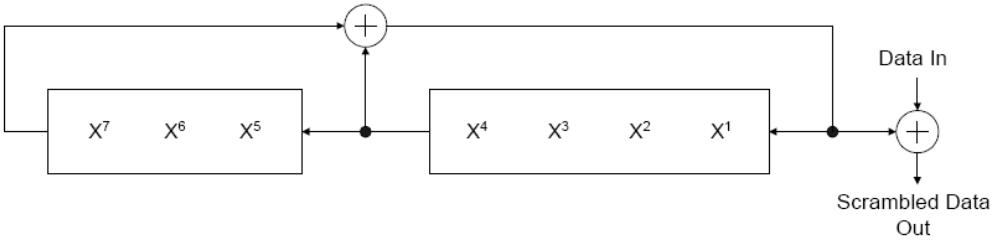


PLC 3G PHYSICAL LAYER DEFINITION - FEC

- **FEC encoder consists of:**
  - Scrambler
  - Reed Solomon encoder
  - For robust mode followed by Convolutional encoder
  - Interleaver

- **Scrambler**
  - helps to give to the data and the FCH a random distribution
  - stream is 'XOR-ed' with a repeating PN sequence

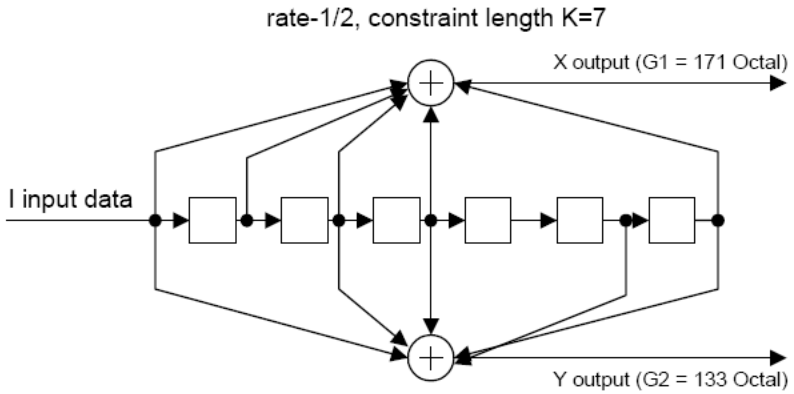
$$S(x) = x^7 \oplus x^4 \oplus 1$$



PLC 3G PHYSICAL LAYER DEFINITION - FEC

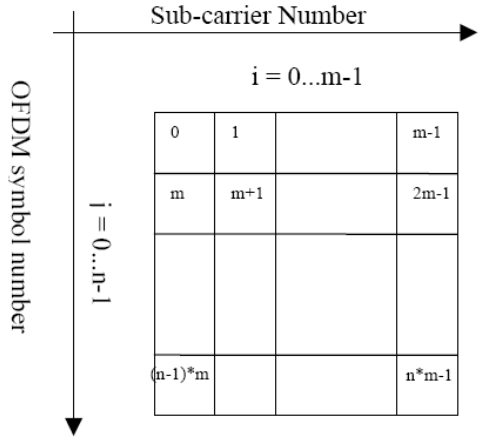
- **Reed-Solomon**
  - shortened systematic Reed-Solomon (RS)
  - Robust mode - RS (N = 255, K = 239, T = 8)
  - Normal mode - RS (N = 255, K = 247, T = 4)

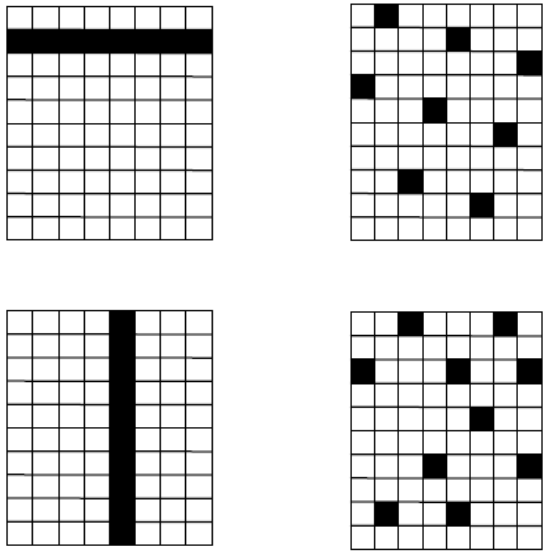
- **Convolutional encoder**
  - Output from RS encoder is encoded again in robust mode
  - tap connections are defined as x = 0b1111001 and y = 0b1011011



PLC 3G PHYSICAL LAYER DEFINITION - FEC

- **Interleaver helps to protect against**
  - burst error which damages a few symbols
  - Frequency deep fade that corrupts a few adjacent frequencies for large num. of symbols
  - In first step symbol data are mixed by circular shift – time dependent noise
  - In second step data with same frequency are mixed by circular shift – frequency dependent noise



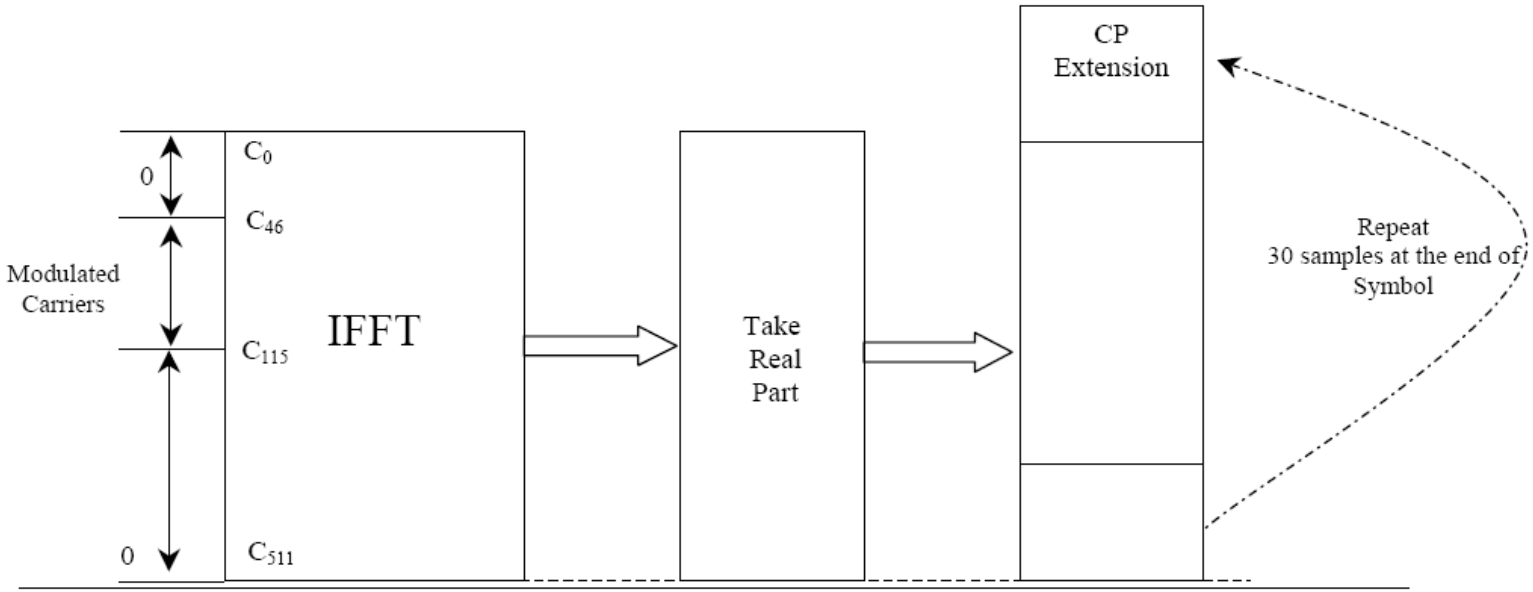


OFDM MODULATOR

- **Modulation mapping:**
  - Each carrier is modulated with Coherent/Differential Binary or Differential Quadrature Phase Shift
  - BPSK uses pre-defined phase difference
  - Uses 0 and 180 degrees
  - DBPSK, DQPSK, ROBUST phase vector uses the same carrier, previous symbol, as its phase reference
  - first data symbol uses the pre-defined phase reference vector
- **Preemphasis:**
  - Helps to compensate attenuation introduced by communication channel
  - all carriers amplitude should not differ more than +-2dB
  - each carrier use own multiplication factor to keep flatness
  - frequency domain samples of an OFDM symbol are multiplied with 128 real filter coefficients

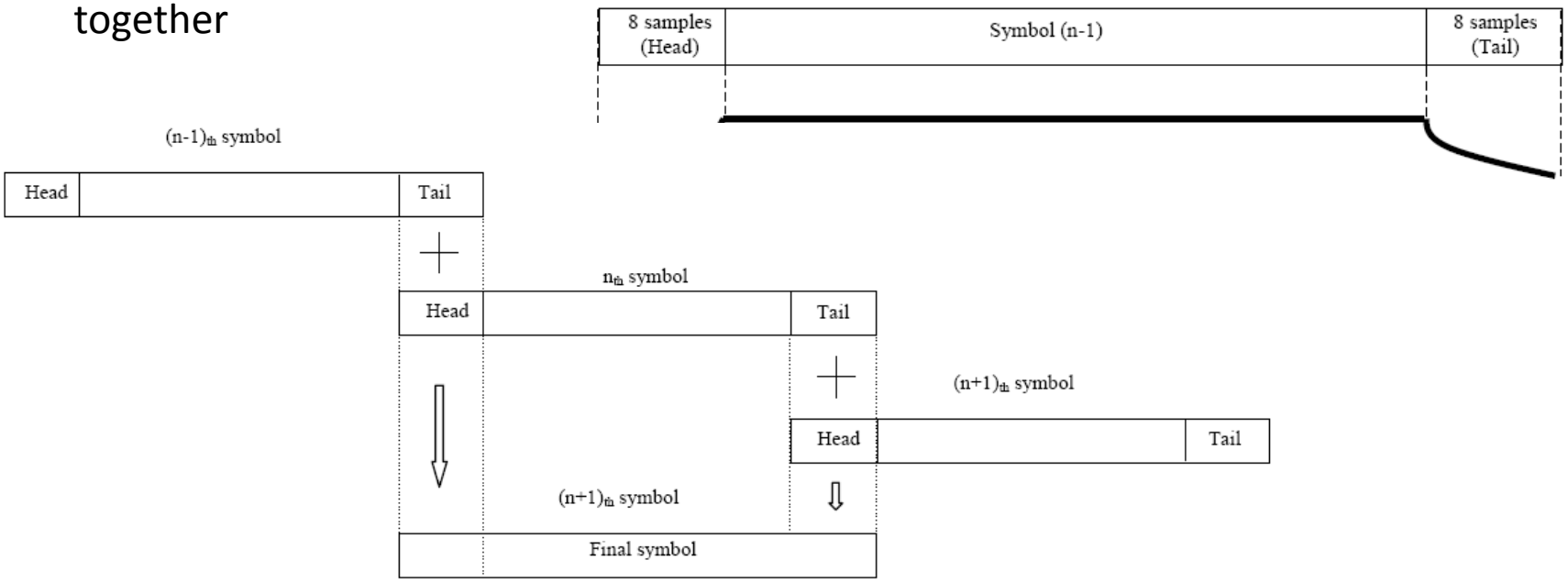
OFDM SYMBOL GENERATION

- OFDM signal is generated by IFFT
- Only real part of IFFT is used



OFDM symbol generation -windowing

- **Windowing**
  - to reduce out of band emmisions
  - Raised cosine window used on each symbol
  - Symbols are overlapped and added together

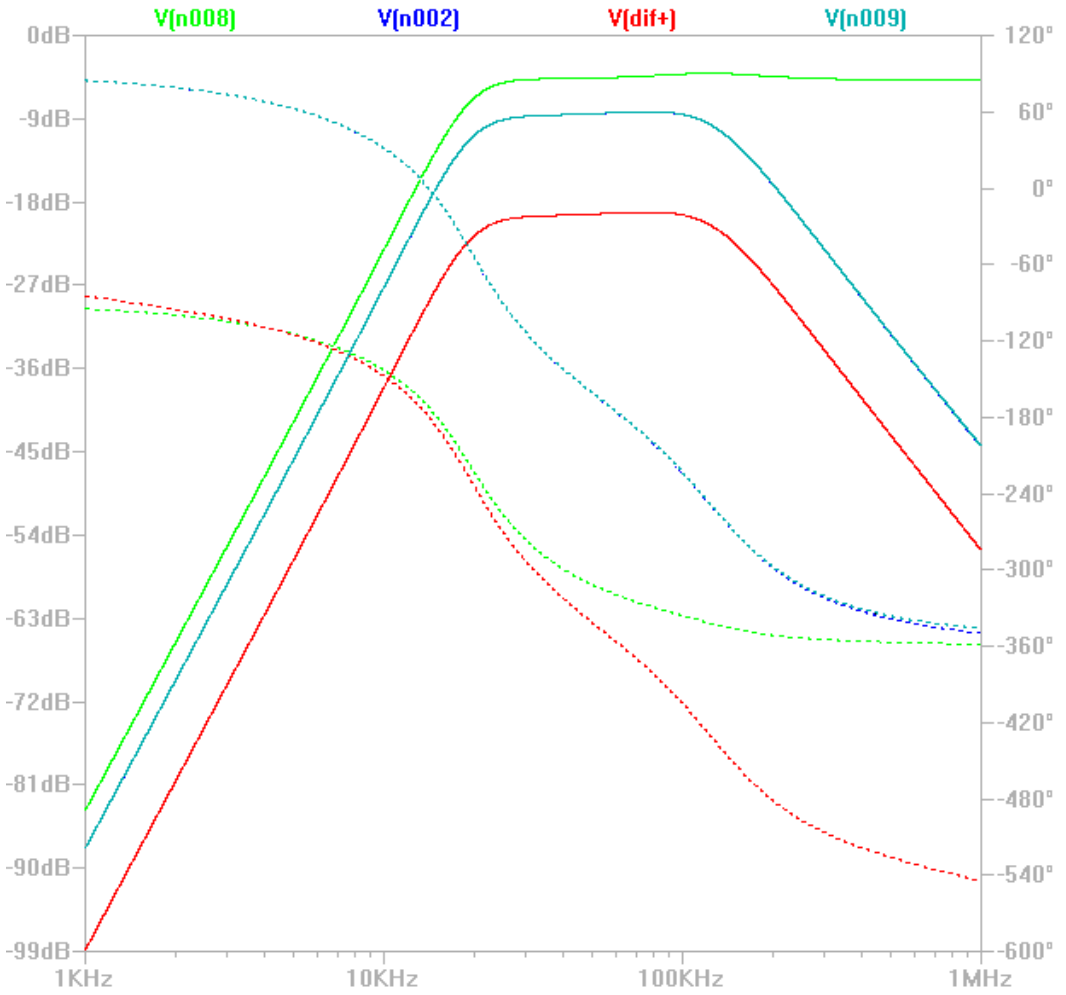


Analog Front End details

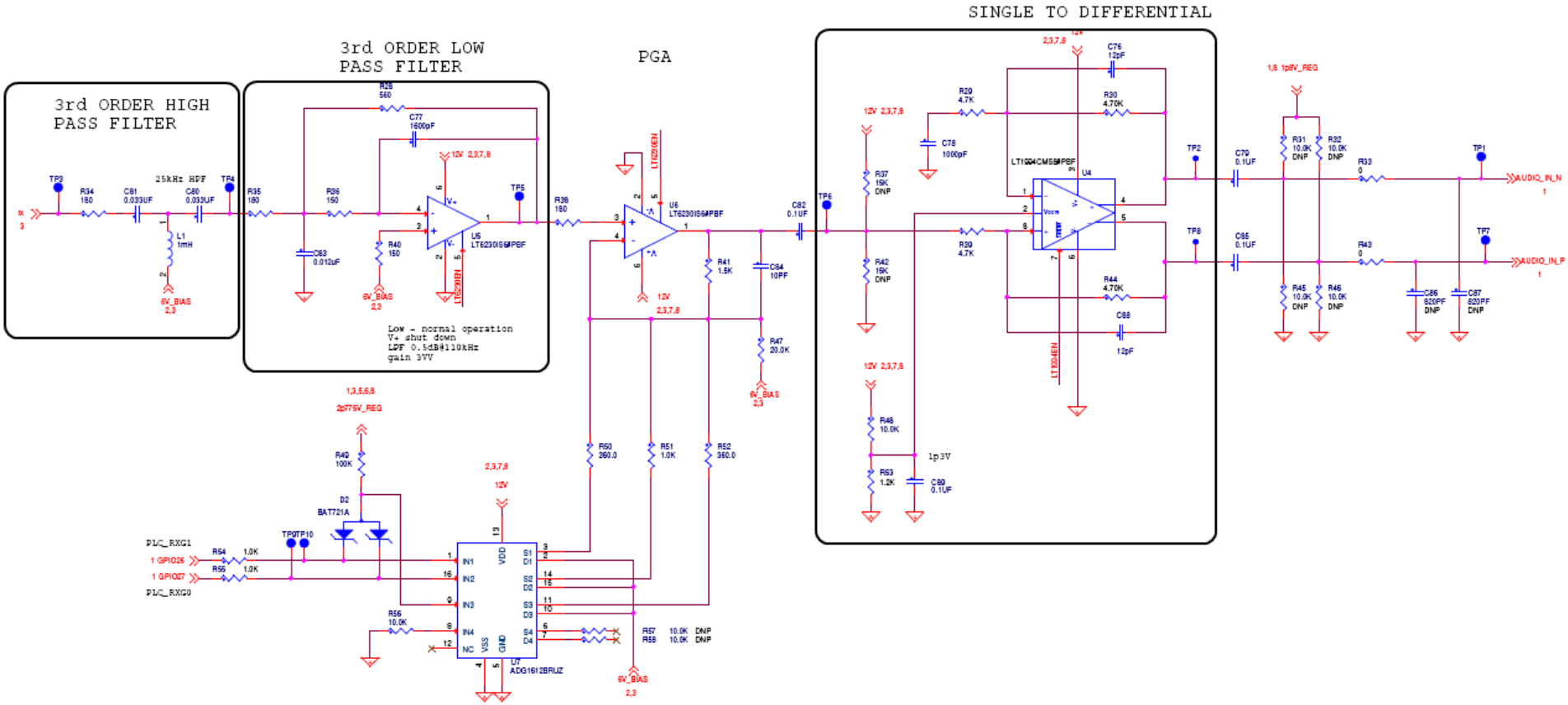
- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- **Analog Front End details**
- existing solution overview
- security short review

Receiver hardware Analogue Front End

- Receiver part consist of
  - passive High Pass Filter (HPF)
  - active Low Pass Filter (LPF)
  - PGA with four steps -10dB, 2dB, 14dB, 26dB total 36dB
  - single to differential converter
  - THD 30kHz to 95kHz 0.1%
  - SNR = 80dB, in freq. range 10kHz to 110kHz @ 500mV
- Receiver ADC should have at least 65 dB @ 400kHz

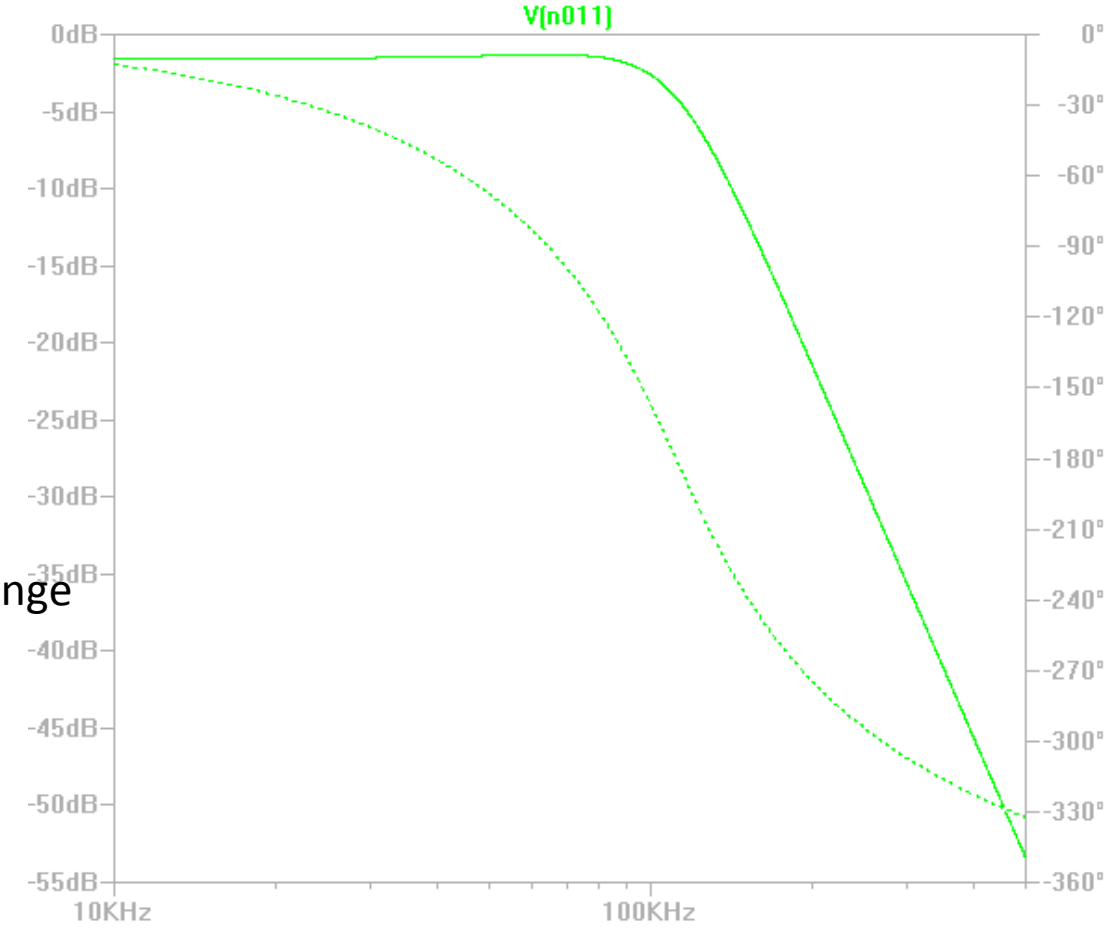


Receiver hardware Analogue Front End

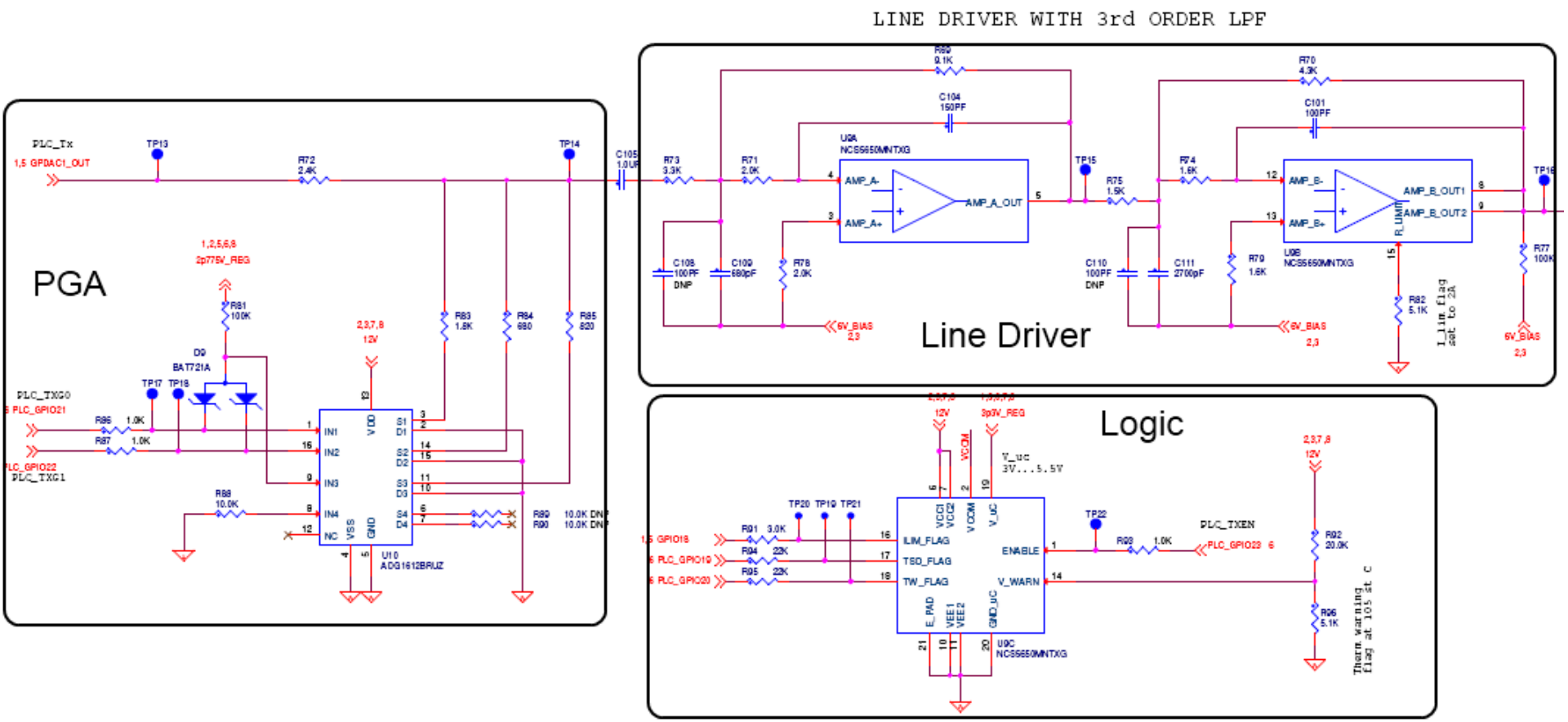


Transmitter hardware AFE

- Transmitter part consist of
  - PGA 0dB, 5dB, 10dB, 15dB
  - Line driver @ 4th order filter to comply CENELEC
  - Logic to Enable/Disable,
  - overheating control
  - overcurrent control
  - 35.9kHz to 90.6kHz frequency range
  - passband frequency is 95kHz,
  - passband ripple 0,5dB

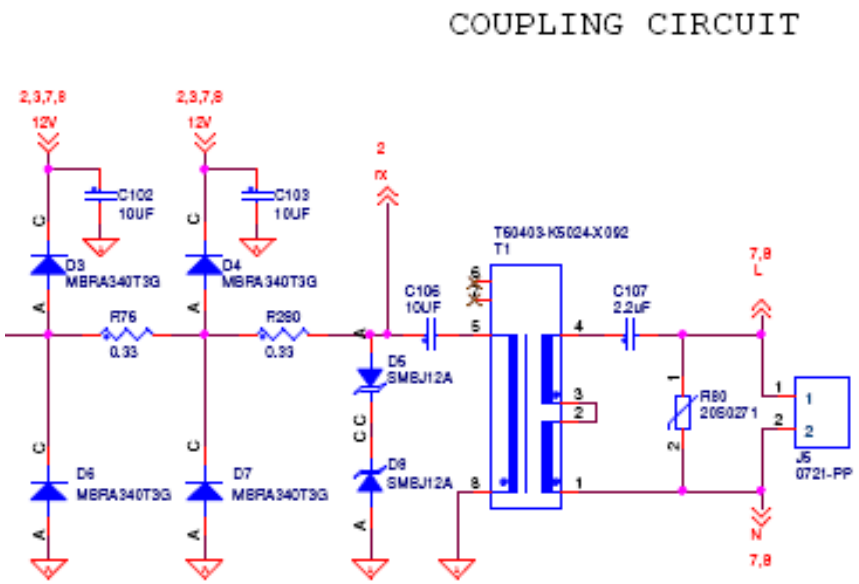


Transmitter hardware AFE



Coupler AFE

- main intent to remove 230V
- no good option for wide band signals
- interface transmitted / received signal with flat response
- protect receiver input and line driver from EMI, hot plug
- coupling impedance < 2 Ohm
- galvanic isolation is more safe



Coupler AFE impedance

- it is hard to achieve good coupling impedance

	2u2	R76, R280 = 0,5Ohm				
f	Load	TP14	TP16	J5	Iload	Zcoupl
f[kHz]	Load[Ohm]	[Vrms]	TP16[Vrms	J5[Vrms]	[Arms]	[Ohm]
35	1,1		3,35	1,15	1,05	2,10
50	1,1		3,48	1,37	1,25	1,69
65	1,1		3,6	1,5	1,36	1,54
80	1,1		3,65	1,6	1,45	1,41
95	1,1		3,5	1,57	1,43	1,35

	1620uF	R76, R280 = 0,5Ohm				
f	Load	TP14	TP16	J5	Iload	Zcoupl
[kHz]	[Ohm]	[Vrms]	[Vrms]	[Vrms]	[Arms]	[Ohm]
35	1,1	na	3,55	0,95	0,9	3,0
50	1,1		3,62	1,17	1,1	2,3
65	1,1		3,78	1,34	1,2	2,0
80	1,1		3,62	1,31	1,2	1,9
95	1,1		3,48	1,27	1,2	1,9

Existing solution overview

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- **existing solution overview**
- security short review

Existing PLC solutions

- Texas Instrument
  - software based modem + analog front end C28x 32-bit CPU 60MHz
  - supports software libraries for S-FSK, G3, PRIME,
- Maxim Integrated
  - chipset solution MAX2992
  - G3 OFDM modulation
- ST - ST7590 specialized system on chip DSP + 51 Core
  - turn - key firmware for OFDM with 96 sub carriers
  - DBPSK, QDPSK, 8DPSK
  - up to 128kbps, Viterbi decoder
  - receiver, transmitter integrated

Security short review

- Smart Grid - general overview
- Smart grid
- what smart grid is, grow drivers
- smart grid elements, standards, regulations, freq. and data rates
- power line transmission channel definition
- S-FSK modulation details
- OFDM modulation details and G3 protocol details
- Analog Front End details
- existing solution overview
- **security short review**

Industrial Trends Drive System Security Trends

Legacy Systems

- ***Closed Networks***
  No connection to outside world
- ***Proprietary Networks***
  Fieldbus protocols
- ***Hardware Control***
  Physical hardware difficult to tamper
- ***Local Access***
  Operator beside the machine
- ***Limited Tampering***
  Fewer attempts to interfere with critical infrastructure

Present Systems

- ***Open Networks*** Connected to global communications network for remote access
- ***Standard Networks***
  Industrial Ethernet protocols
- ***Software Control***
  Easier to tamper with less obvious impact
- ***Remote Access***
  Operator connects via wired of wireless from distant location
- ***Increased Tampering***
  More frequent attempts to interfere with critical infrastructure, e.g. electric utilities, water treatment and transportation systems

Rapidly Rising System Security Requirements

Prevent Tampering

- ***Critical Control***
  Maintain predictable control of critical infrastructure
- ***Functional Safety***
  Maintain safety system integrity
- ***Unauthorized Access***
  Secure data storage for master data and network session encryption keys
- ***Secure Boot***
  Start from a trusted code base or don't start at all
- ***Threat Detection***
  Detect both physical and network attacks

Protect Intellectual Property

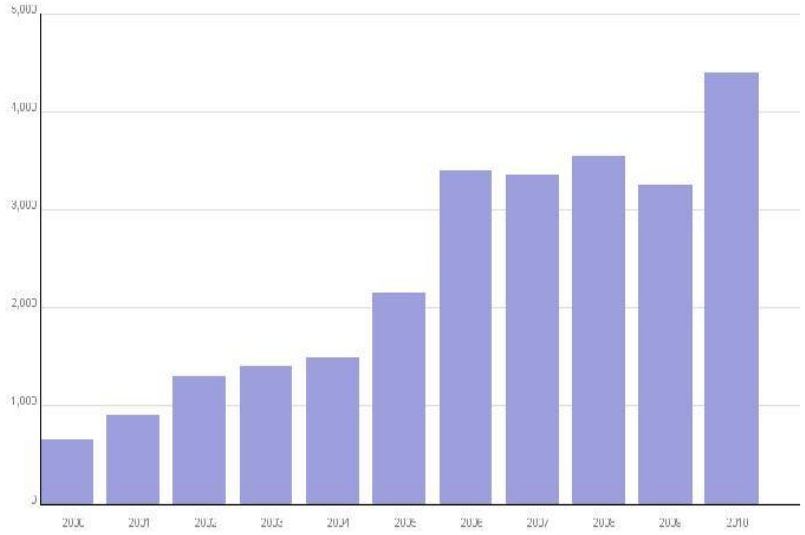
- ***Product Cloning***
  Avoid the loss of product differentiation through reverse engineering, duplication, and unapproved inter-operability
- ***Data Theft***
  Secure storage of sensitive data
- ***Secure Debug***
  Remotely debug and update software code in a trust environment

Cyber crime cost the UK an estimated 27B Pounds a year, and as much as US$1Trillion a year globally.

Nov 14, 2011
London Conference on Cyberspace
Britain Prime Minister David Cameron

Need for Security in the Electricity Grid Infrastructure

- Grid infrastructure is one of the key assets for any nation
- Dramatic increasing in number of identified system vulnerabilities
- Increasing number of attempted and successful attacks on the grid/metering systems
- Protection through Anonymity is no longer an option!
- Smart grid infrastructure is about connectivity making it attractive for hackers (curious and malignant)



36% increase in vulnerabilities in 2010 compared to 2009.
Source: IBM X-Force Research and Development team

Smart Grid Vulnerability types and trends

Increasing number of new vulnerabilities

- Operational systems – generators, transformers, Supervisory Control & Data Acquisition (SCADA) Systems & Energy Management Systems (EMS), programmable logic controllers (PLCs), substations, smart meters, and other intelligent electrical devices (IEDs) which control the generation and flow of power
- IT systems – PCs, servers, mainframes, applications, databases, billing management systems, web sites, web servers, web services, etc.
- Communications networks and protocols – Ethernet, Wi-Fi, Zigbee, 3G/4G, DNP3, IEC 61850, Power Line Communications
- Communications disruptions and introduction of malicious s/w or compromised h/w can result in DoS
- Increasing End points – smart meters, EVs, smart phones and other mobile devices, home appliances?
- Human factors – lack of training and awareness, social engineering attacks, phishing attacks, misuse of USB drives, etc.
- Intentional, Terrorist, Industrial Espionage, Malicious, Accidental, Inadvertent
- Malware: Rootkits, trojans, viruses, worms, keyloggers, bots,.Risk enhanced by rich & open OS

  Countermeasures: trusted execution, high assurance boot
- Hacking: Reverse engineering, brute force

  Countermeasures: secure storage, secure debug, encryption
- Physical attack: Bus snooping, glitching,

  Countermeasures: secure storage, tamper detection

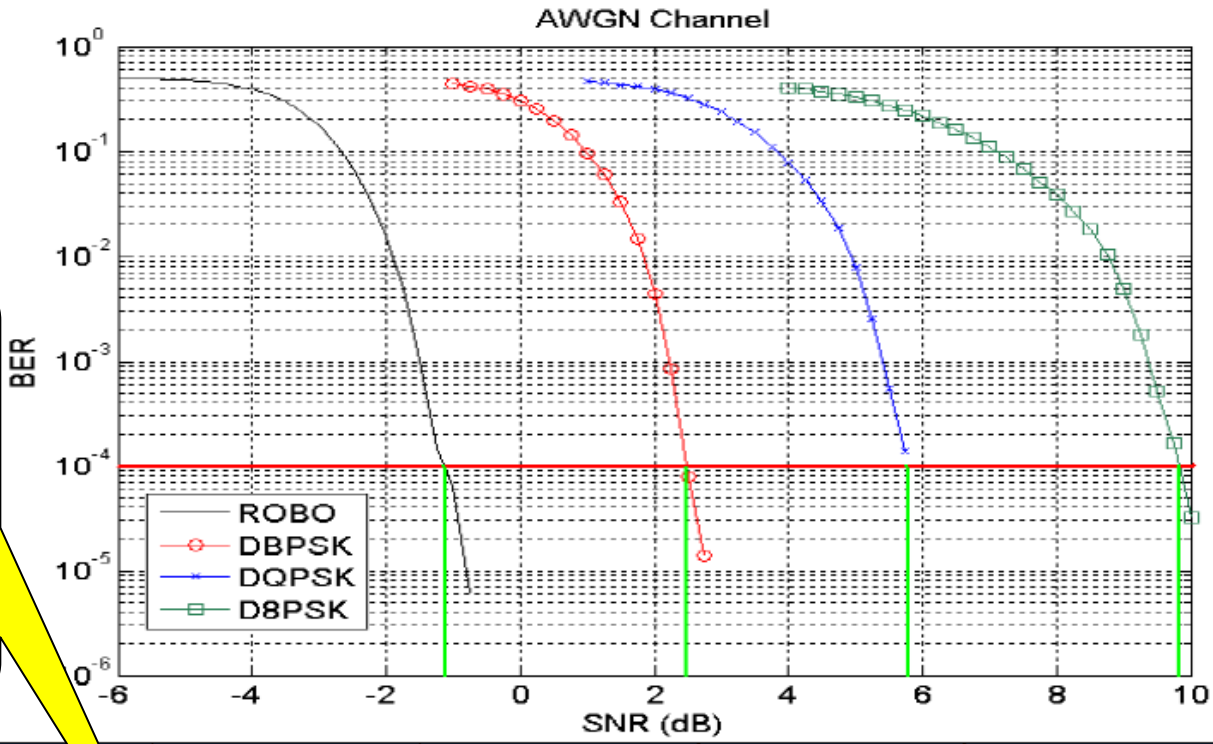
Security standards in EMEA

- Standards bodies like CEN/CENELEC/ETSI/ENISA coordination group for Smart Grid are working on the ongoing initiative for a European smart grid standard architecture.
- Will publish a standard architecture by the end of 2012.
- It is expected to have the final technical report approved by Member States by the end of this year.
- Different granularity levels, ranging from a conceptual (block diagram) and/or functional architecture to a detailed architecture (including blocks and interconnections) for each one of the general blocks.
- Based on 400 use cases, on existing standards, and will also include security issues.

THANK YOU

BACKUP SLIDES

G3-PLC Data Robo vs. Speed



AMI needs data. Slow is good

Frequency Band	Typ Robo Data Rate (bps)	Typ DBPSK Data Rate (bps)	Typ DQPSK Data Rate (bps)	Typ D8PSK Data Rate (bps)	Max D8PSK Data Rate (bps)
CENELEC A (36kHz to 91kHz)	4,500	14,640	29,285	43,928	46,044
FCC (150kHz to 487.5kHz)	21,000	62,287	124,575	186,863	234,321
FCC (10kHz to 487.5kHz)	38,000	75,152	150,304	225,457	298,224

G3-PLC DATA ROBO VS. SPEED

- **PLC2+ (ZA ST-7538 and many others)**
  - Robo mode, Multi channel FSK with band in use ISP. **1.2k baud**, FSK to IEC 61334-5-1
- **PLAN+ (ErDF ST-7570 and many others)**
  - 300k pilot of IDIS compliant "Linky" meters. **2.4k baud**, S-FSK to IEC 62056-8-3

- **SITRED (Enel/Endesa: ST-7580) Proprietary**. Announced on 5 Oct 2009
  - Uses B-PSK, Q-PSK or 8-PSK in Cenelec A, B or C bands to achieve **28k baud**
- **PRIME (Iberdrola ST-7590)** Launched on 13 Sept 2007
  - Iberdrola appointed as coordinator of the **EU open meter project,** launched on 28 Jan 2009
  - OFDM MAC and PHY layer specifications made publically available on 28 Feb 2008
  - 96 sub-carriers in Cenelec A band (42 to 89kHz) achieves **128k baud**
  - IEC 61334-4-32 data link layer. LV network only. Interop tests (3 vendors) done 31 July 2008
  - + **G3 PLC (ErDF Maxim G3, Sagem) High probability most of ErDF 35m will be PLAN+**
  - ErDF and Sagem joint development. Should not be confused with ERDF PLAN+ pilot
  - Designed for robustness, PLAN/PLAN+ coexistence (via notch filters), **MV/LV crossing**
  - 6loWPAN/IPv6 convergence layer. IEEE 802.15.4 MAC achieves **300k baud** with FCC/D8PSK
  - 7 vendors engaged in interoperability tests. Cenelec A band "ROBO" mode runs at **4.8k baud**
- **IEEE P1901.2 (NIST PAP15 TI F2806x, MC13260, EV8000)** Co-developed with ITU-T G.hnem
  - Programmable OFDM (software defined radio). FCC/QPSK achieves max of **800k baud**
  - Caters for alternate MAC/PHY layers (Prime, G3). G.cx coexistence scheme defined
  - Requirements of SAE J2931 PLC for EV charging and AHAM appliance control being considered
- **Next Generation PLC** Grid **Analytics** (pilot projects up and running), **Diversity** to avoid jamming

120 - Landis+Gyr, PLC – Guide for AMI use in Africa

G3-PLC DATA ROBO VS. SPEED

Factor	433 MHz	868 MHz	2.4 GHz
	Attenuation	Attenuation	Attenuation
Open office	0 dB	0 dB	0 dB
Window	< 1 dB	1 – 2 dB	3 dB
Thin wall (plaster)	3 dB	3 – 4 dB	5 – 8 dB
Medium wall (wood)	4 – 6 dB	5 – 8 dB	10 – 12 dB
Thick wall (concrete)	5 – 8 dB	9 – 11 dB	15 – 20 dB
Armoured wall (reinforced concrete)	10 – 12 dB	12 – 15 dB	20 – 25 dB
Floor or ceiling	5 – 8 dB	9 – 11 dB	15 – 20 dB
Armoured floor or ceiling	10 – 12 dB	12 – 15 dB	20 – 25 dB
Rain and/or Fog	20 – 25 dB	25 – 30 dB	?? *

121 - Landis+Gyr, PLC – Guide for AMI use in Africa