Current anti-tamper techniques used in consumer and light industrial electrical energy meters

Steve Underwood, MSP430 Marketing, Hong Kong

Anti-tamper techniques in electrical energy meters

- Traditional electricity meter designs have no ability to detect or deal with tampering.
  - They measure power based only the voltage between the two inlet terminals, and the current flowing between the live inlet and outlet terminals.
  - They may be largely unscreened.
  - Some forms of tampering are easy for even unsophisticated people to implement, and hard to detect.
- Various markets now require some forms of anti-tamper measures, and the list is growing.
- Each year new anti-tamper measures are being introduced.

Anti-tamper techniques in electrical energy meters cont…

- Many tampering scenarios are documented.
  - Some are quite easy to implement, and hard to detect.
  - Some seem hard to implement, and seem unlikely to be used. Utilities are still interested in protecting against them.
- Various methods of tampering are possible.
  - Physically tampering with the meter.
  - Magnetic interference.
  - Adding new wires to bypass some current.
  - Moving or removing existing wires.
  - Adding some simple components - diodes, resistor, capacitors (generally in combination with moving wires).
- The single phase and 3-phase markets differ.
  - Single phase anti-tamper is a well developed market.
  - 3-phase anti-tamper features are just starting to grow.

Physically tampering with the meter.

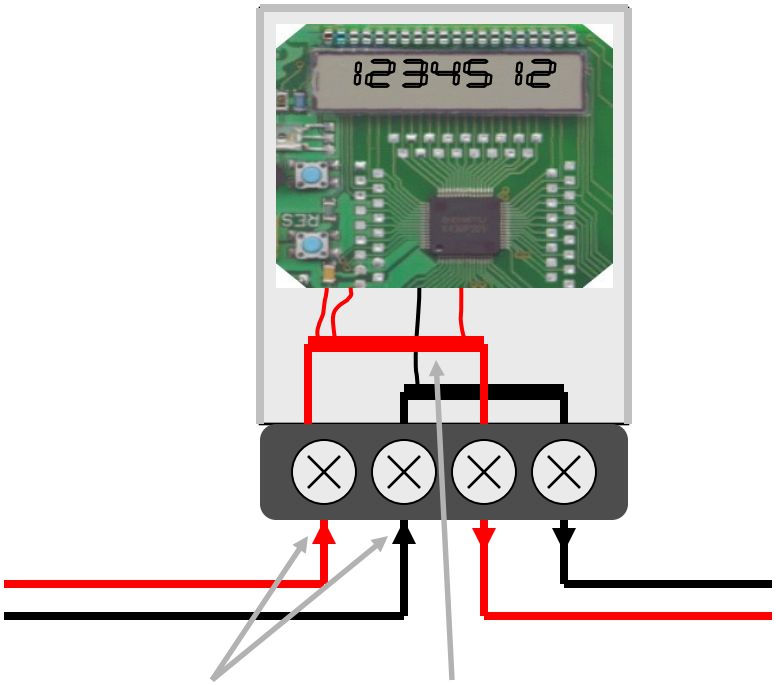
- The meter's case is the first line of defence.
- Some utilities demand polycarbonate cases.
  - The case may be the most expensive component.
  - Compact electronics can allow, compact cases, which can save significant cost.
  - Some utilities require secondary cases to give greater isolation of the parts vulnerable to tampering.
- Many utilities have detailed specifications for how the case must be sealed.
  - They usually require some form of factory seal.
  - Some require the case be physically damaged to open it.
  - Some meters are now welded shut.

Physical tampering with the meter cont…

- Many utilities demand the case must be opened to initiate recalibration.
  - Meters offering fully automated calibration through communications ports, may require an internal "calibration jumper".
- The design of the terminal block cover can help reduce simple fraud.
  - Most utilities require the terminal block cover have some form of seal.
  - Avoid spaces around the wires, where metal objects might be inserted.
  - Some utilities require an intrusion detector on the terminal block cover.

Meters without tamper resistance measures.

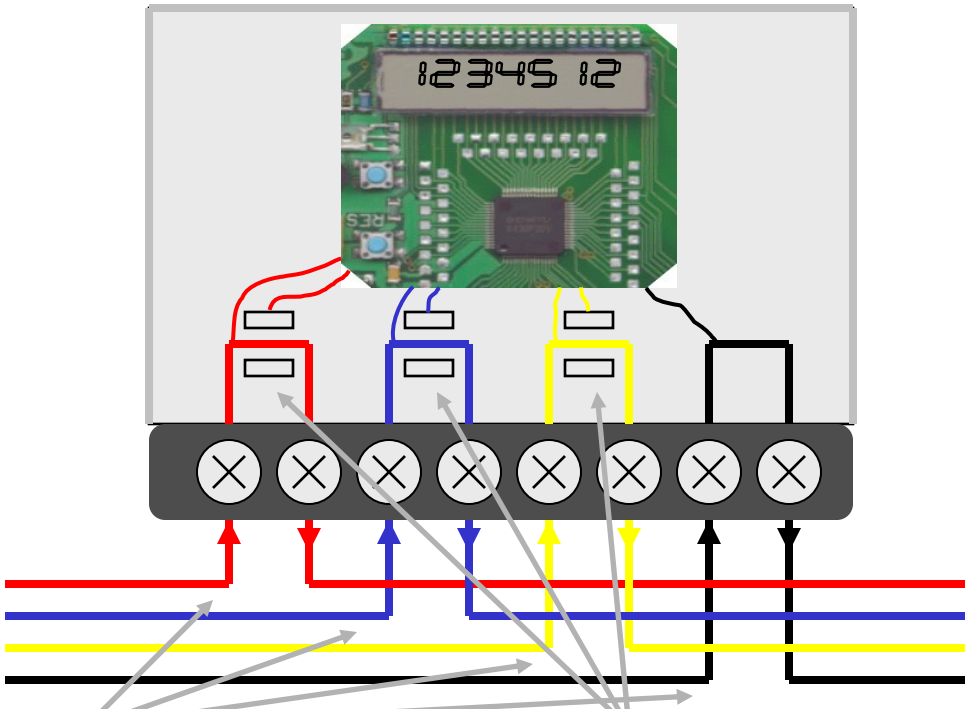
Simple single phase meter



Voltage is sensed between the input terminals.

Current is sensed as the voltage across a shunt resistor.

3 phase meter with only internal sensors.

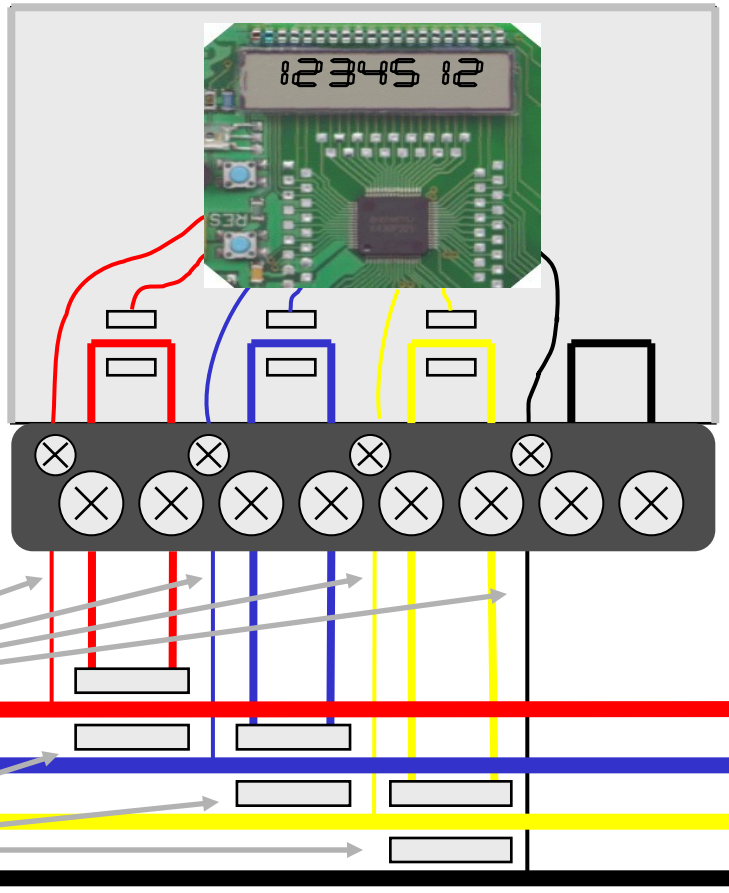


Phase voltages are sensed between the phase input and neutral terminals.

Phase currents are sensed with current transformers.

Meters without tamper resistance measures.

3 phase meter with external multiplier CTs



Separate terminals are used to measure the phase voltages.

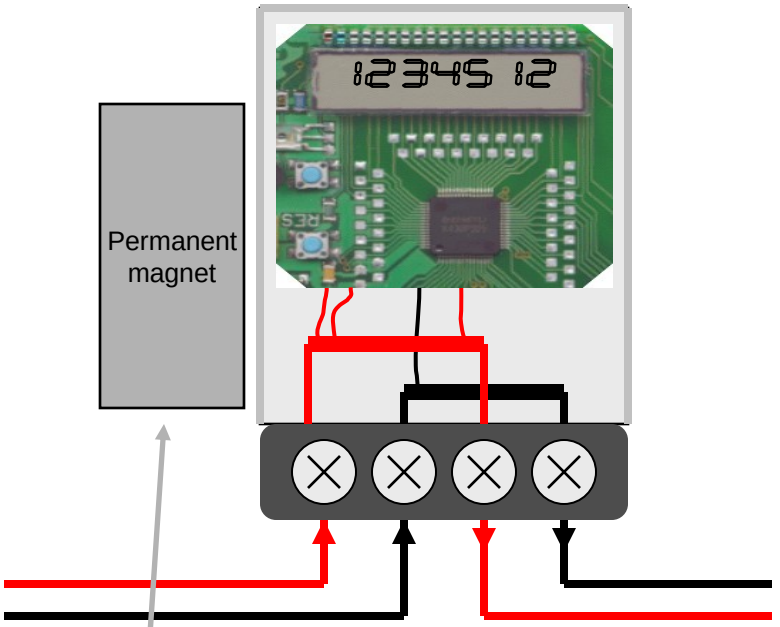
External multiplier CTs are used to measure large currents.

Magnetic interference.

- Both static and alternating magnetic fields might be used to affect a meter's operation.
  - Powerful permanent magnets against the meter's case.
  - Large coils generating strong alternating fields.
- Strong external static magnetic fields can saturate transformer cores, or stop electromechanical counters.
  - Powerful permanent magnets attached to the case of a meter can stop a transformer based power supply dead.
  - They can reduce a CTs current output to near zero.
  - The range of the magnet's effects is small.
  - The location of CTs within the case can help considerably.
  - 0.2T tolerance used to be demanded. 0.5T or 0.8T is now more common.
  - It is **hard** to shield a CT against 0.8T magnets.

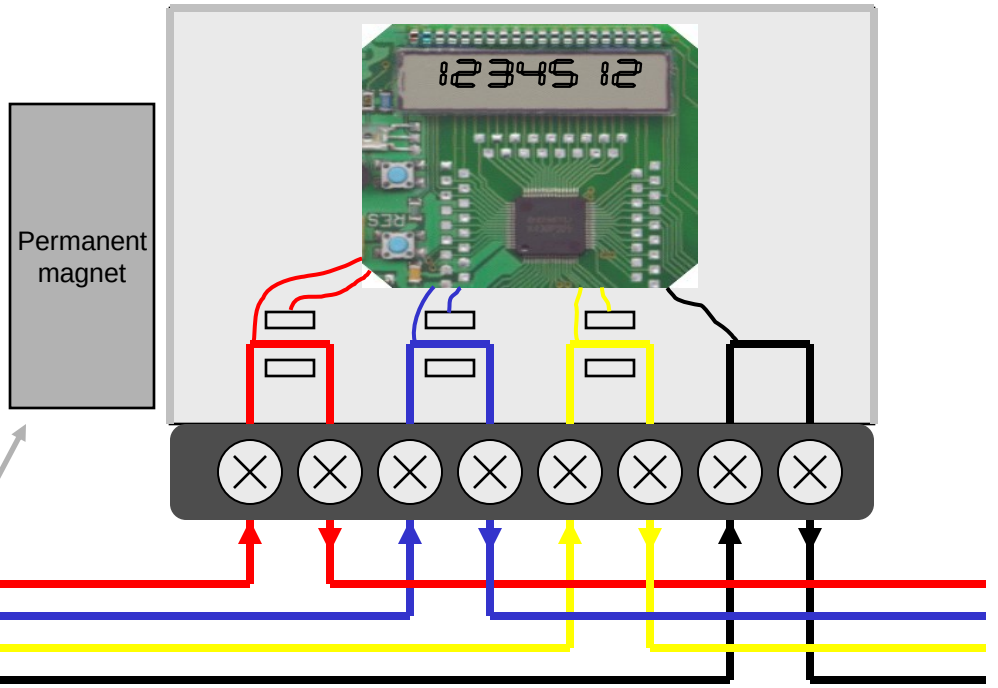
Magnetic interference.

Simple single phase meter



If the power supply uses a transformer, this could shut down the meter.

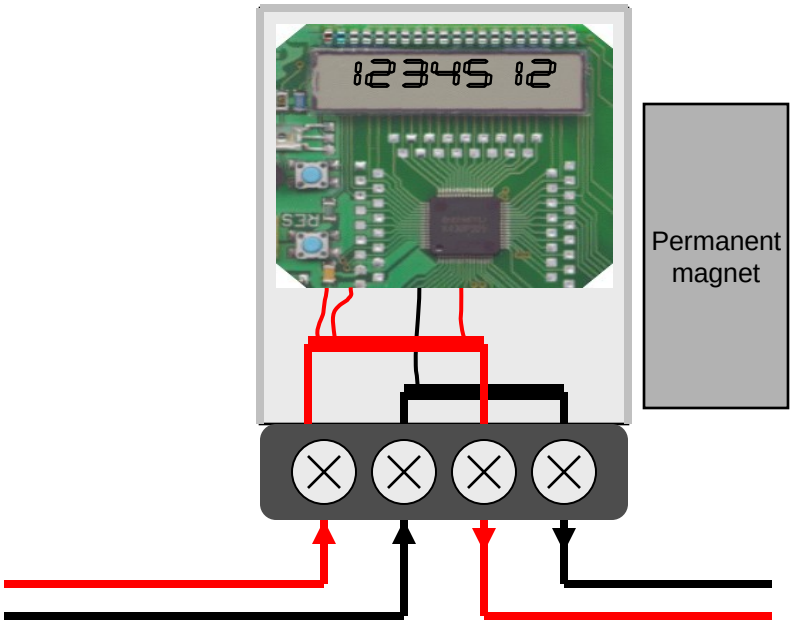
Simple 3 phase meter



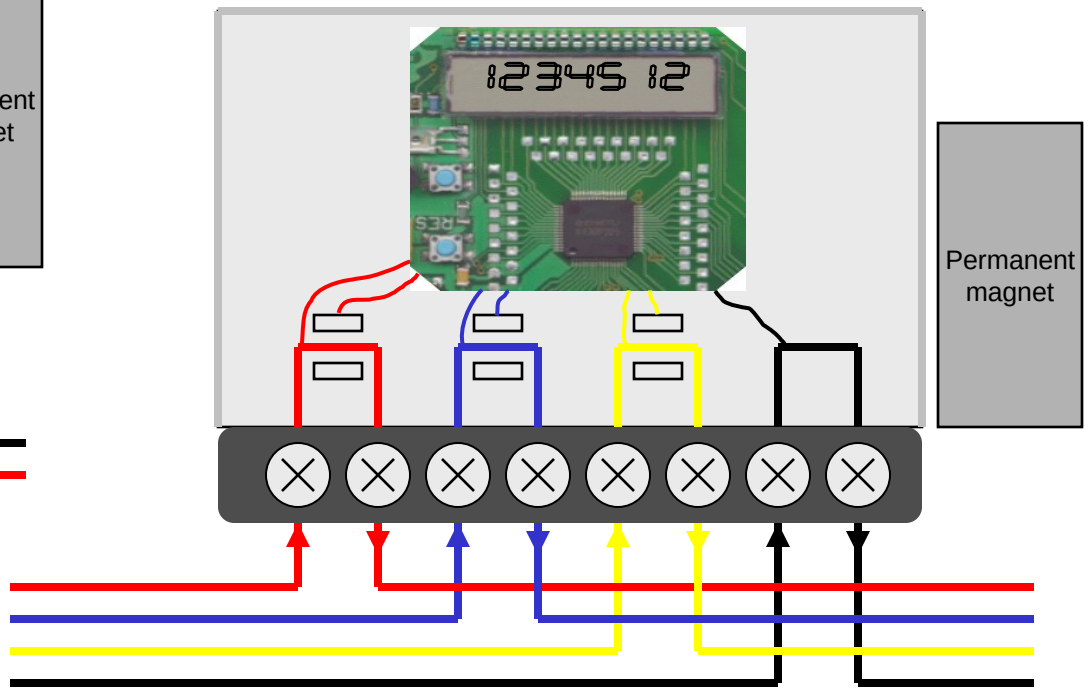
May completely paralyse the red phase CT, yet have only a small effect on the yellow phase one.

Magnetic interference.

Simple single phase meter



Simple 3 phase meter



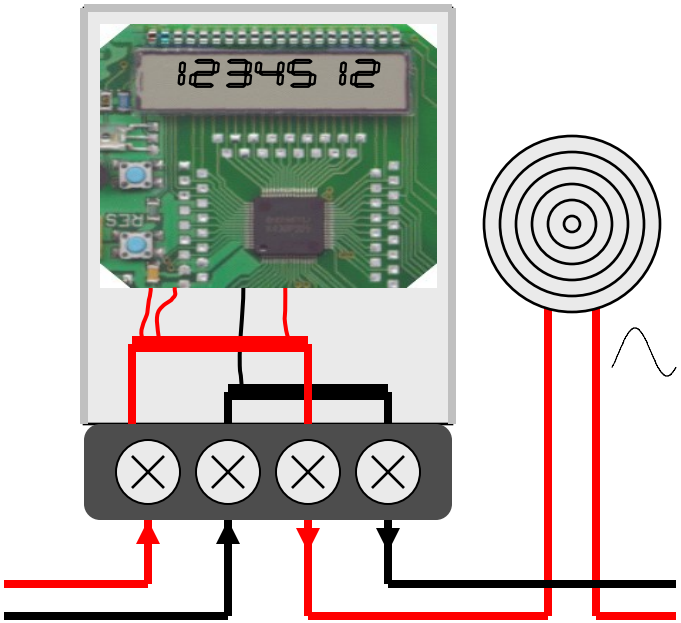
A change of magnet position may greatly alter its effect.

Magnetic interference.

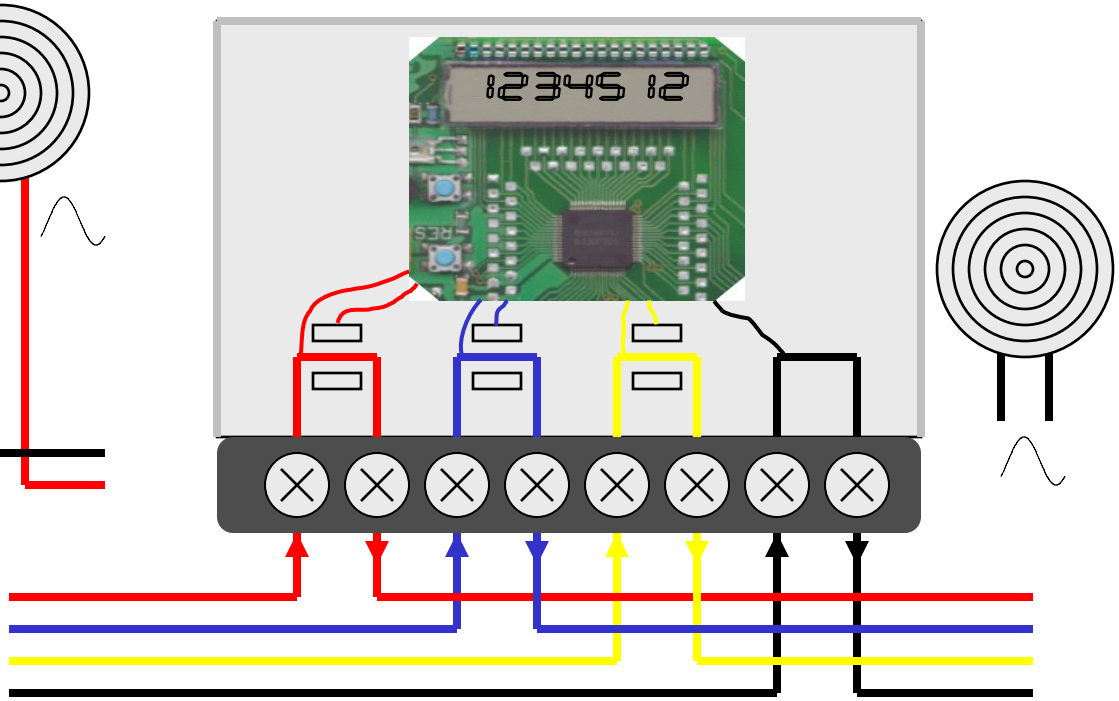
- Sufficiently strong alternating fields can affect most components.
  - Shunt resistors.
  - Current transformers.
  - Rogowski coils, though immune to permanent magnets, are very susceptible to alternating fields.
  - The core electronics.
- Strong alternating fields are a plausible tampering technique, if the meter's load is supplied through a large coil placed near the meter.

Magnetic interference.

Simple single phase meter



Simple 3 phase meter



Magnetic interference cont...

- Location is important.
  - Keep magnetically sensitive devices near the back panel – it is usually harder to tamper behind the meter.
  - Keep sensitive devices away from the top and sides, where it may be easy to attach a large permanent magnet.
- Magnetic screening is important, but imperfect.
  - Steel cases for CTs are the first line of defence.
  - Lining the case with steel is a possible second line of defence.
  - Rogowski coils are immune to permanent magnets, but considered quite hard to screen against alternating fields.
  - The effect of magnets on electromechanical counters is major reason for the growth of LCD meters.

Magnetic interference cont...

- Fields of 0.5T or more are hard to effectively exclude from magnetically sensitive components.
  - Transformer based power supplies are very problematic.
  - CTs can be greatly affected.
- All shunt current sensor solutions might help, but…
  - Using shunt circuits on multiple phases without isolation is hard.
  - Isolating optically is expensive.
  - Isolating with potential transformers introduces more magnetically susceptible components.
- If you can't keep the magnetic field out, measure it and take special action.
  - Low cost, Hall effect, magnetic sensors may be used to detect strong fields, and charge the subscriber at a very high rate.
  - Has a patchy history because of abuses, but is now in some standards.

Magnetic interference cont...

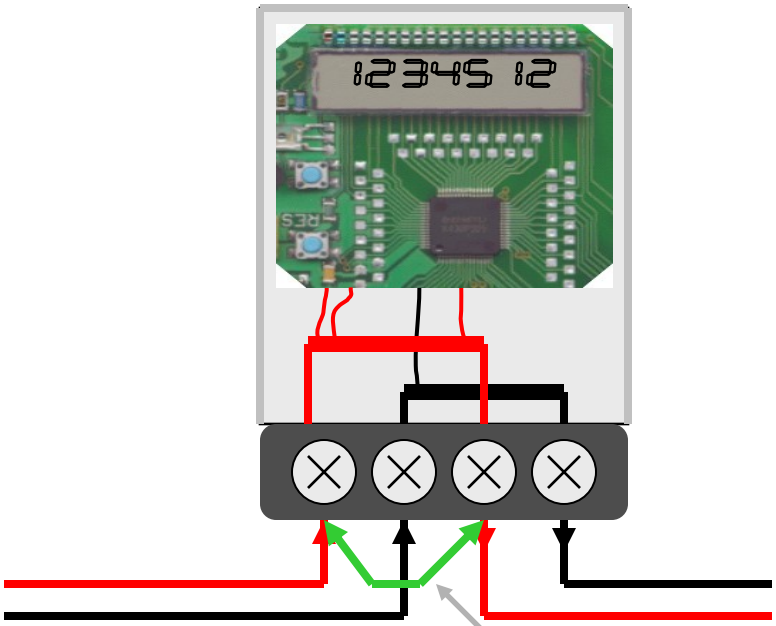
- RC power supplies avoid magnetically susceptible components.
  - Only a few markets require electrical isolation (China is the main one).
  - RC power supplies are the best solution, where electrical isolation is not required.
  - If the power consumption of the meter is large, RC supplies get hot, and total consumption may not meet the spec.
  - High harmonic energy can greatly increase dissipation in the "R" of the power supply.
  - Ultra low power devices **(e.g. MSP430)** solve this.
  - A 2.5W resistor runs cool under normal conditions, and not too hot under the worst harmonic conditions.

Unbalanced current tampering

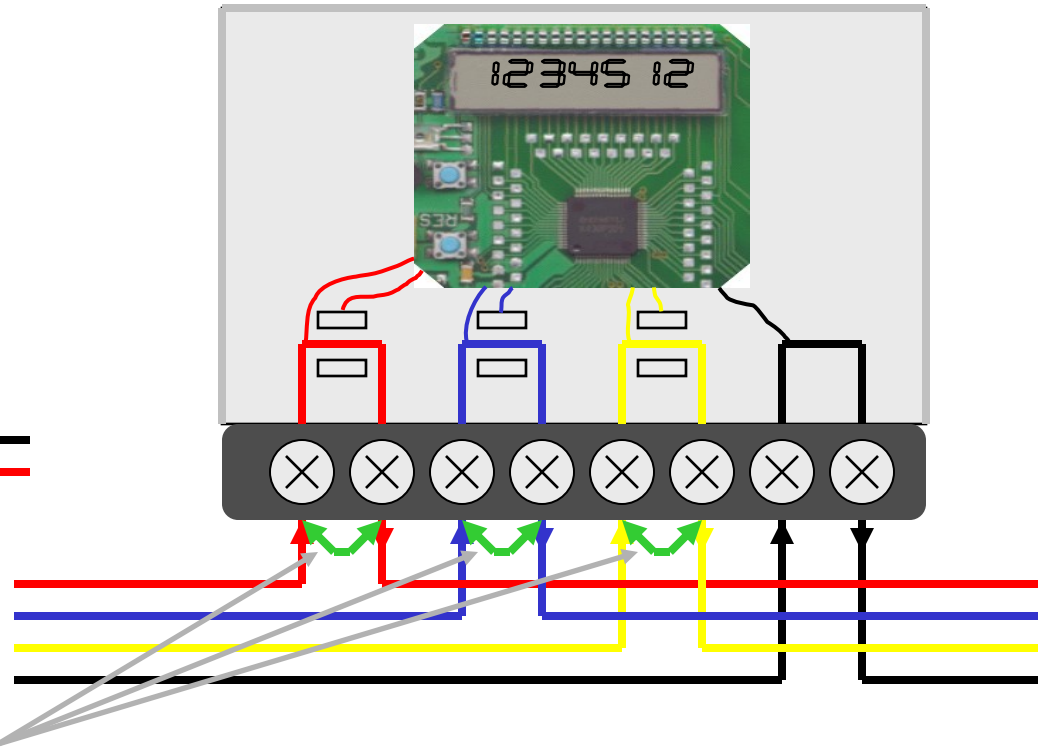
- Often called earthed mode, but applies to any imbalance between the load measurable in the live and neutral leads.
- Tamperer tries to bypass some of the current, and make the meter read less than the true power.
- Can be as simple as a piece of metal wedged against the terminal block of the meter.
- Easily implemented by unsophisticated people.
- Often hard to physically detect.
  - Changes may be easily removed in seconds when someone calls to read the meter.

Unbalanced current tampering cont…

Simple single phase meter



Simple 3 phase meter



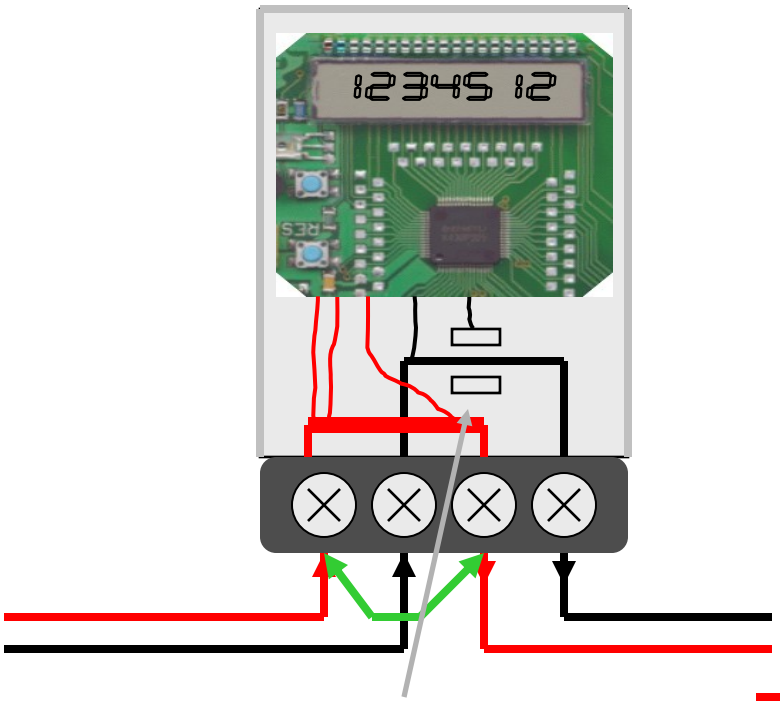
Metal objects pushed against the terminal block bypass a substantial percentage of the current.

Unbalanced current tampering cont…

- Detecting imbalance adds significantly to the cost of the meter.
  - Requires an additional current sensor.
  - The first single phase sensor may be a low cost shunt resistor, but the extra sensor is normally a more expensive CT, for isolation reasons.
- General single phase strategy is to measure power from both the live and neutral leads, and look for balance.
- 3 phase meters can monitor the neutral lead current.
- Balance is usually very good, as earth leakage currents should be very small.
- Meters are usually expected to achieve the same accuracy measuring through either lead.

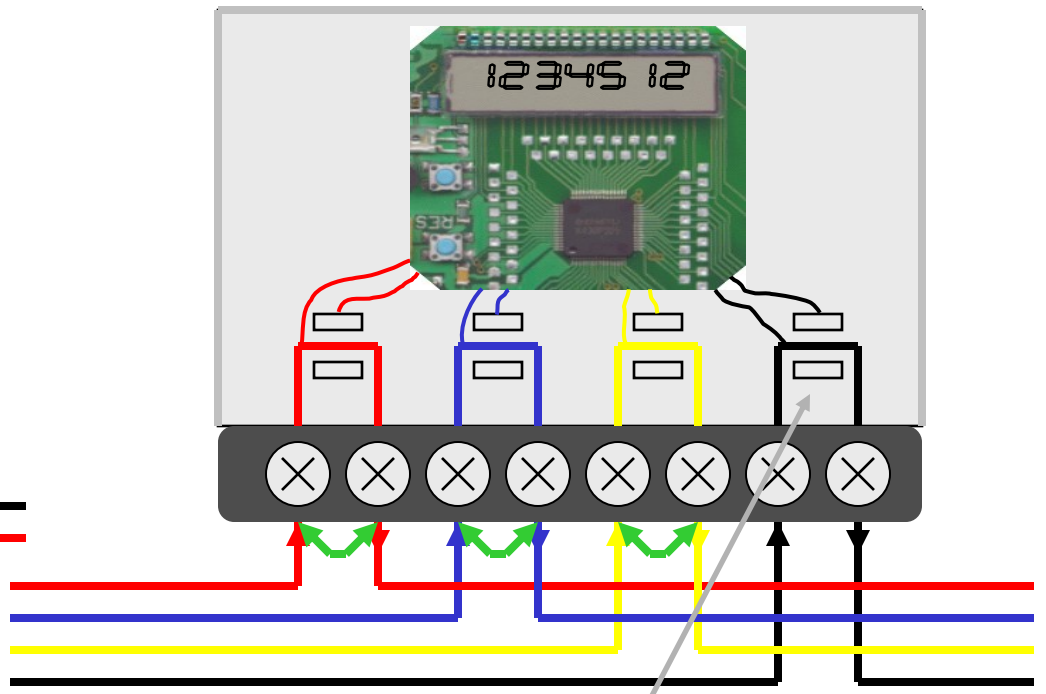
Unbalanced current tampering cont…

Single phase meter



Extra CT to monitor whether the neutral current matches the live current.

3 phase meter

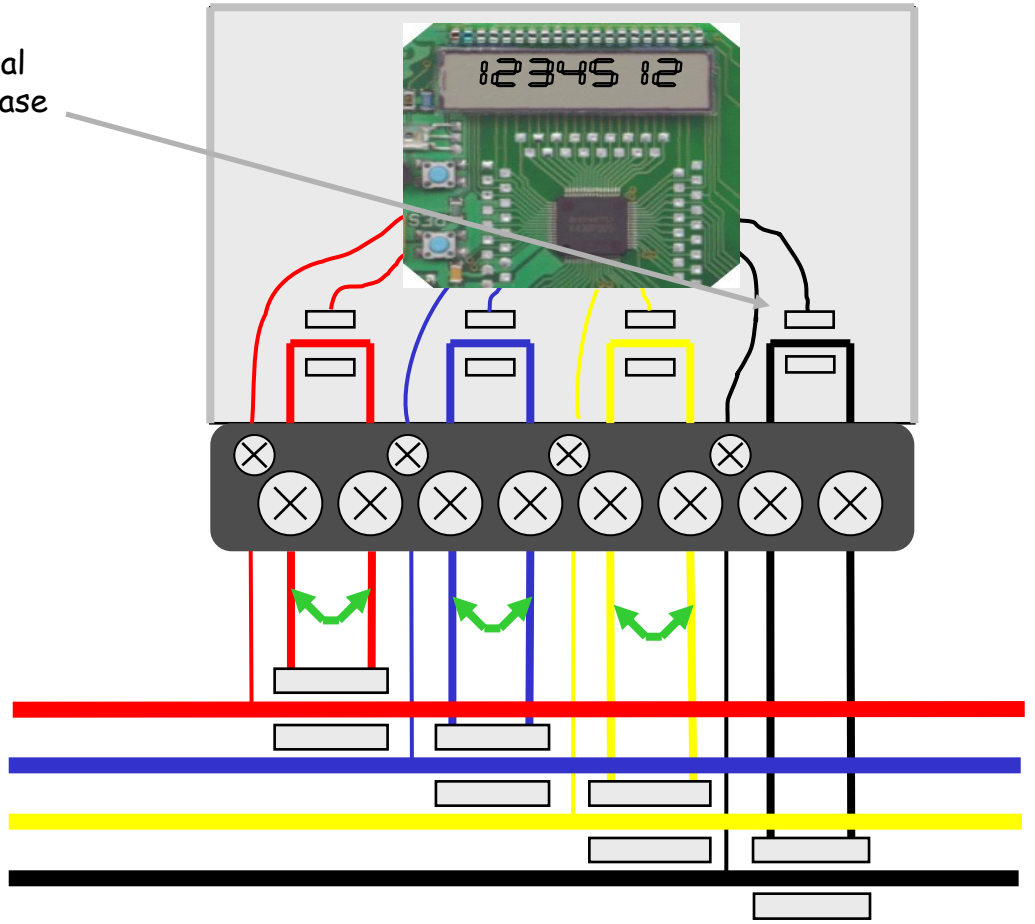


Extra CT to monitor whether the neutral current is consistent with the three phase currents.

Unbalanced current tampering cont.

3 phase meter with external multiplier CTs

Extra CT to monitor whether the neutral current is consistent with the three phase currents.



Current may be bypassed, by slitting the insulation and attaching bypass leads. This can be very hard to see.

Unbalanced current tampering cont…

- Care is needed, so EMI conditions do not cause false detections of imbalance.
  - Problem is greatest at small power levels.
  - Persistence checking and careful choice of thresholds may be needed.
- Tamperers may try to bypass both leads.
  - Using a small imbalance threshold makes this harder.
  - Utilities want the smallest threshold possible.
  - False triggers must be avoided.
  - 12.5% (i.e. 1/8th) difference is a common criterion.
  - Using a smaller difference (e.g. 1/16th or 1/32nd) at high current, and a wider difference at low current works well.

Unbalanced current tampering cont…

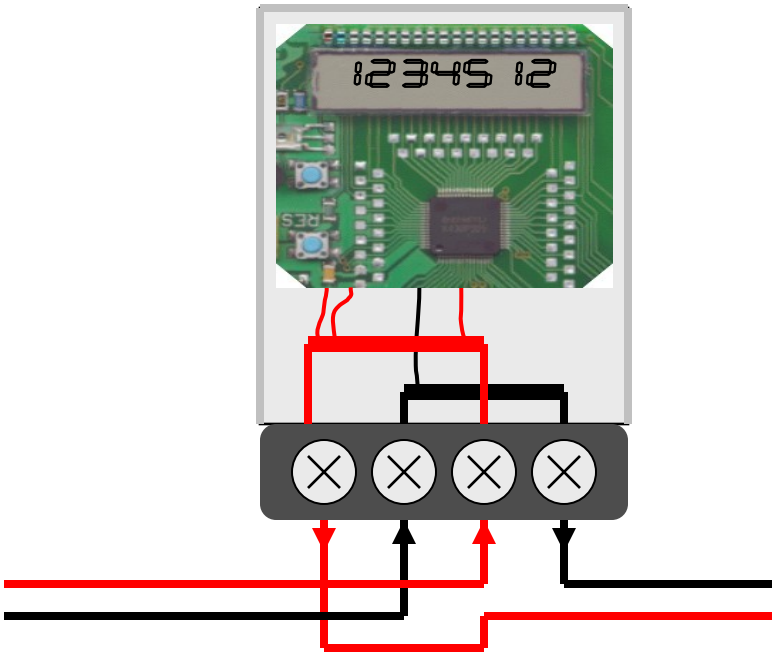
- Usually biased towards using the reading from the current in the live wire.
- Meters usually have an "Earthed" indicator.
  - Typically an LED.
  - Moving toward the use of LCD segments to lower cost.
- Meters may record the time and duration of periods when imbalanced is detected.

Reverse current tampering

- Connections may be reversed, in an attempt to make the meter count backwards.
- Much more invasive than bypassing current.
  - Requires actual rewiring of the meter.
  - Cannot be undone in 5 seconds when a meter reader calls.
  - Cannot be left permanently in place, or the meter will read less than zero.
- May still be hard to physically detect when reading the meter.
  - Meters are typically in cramped spaces.
  - It may be hard to see where the wires go.
- Generally, no extra components are needed for detection.

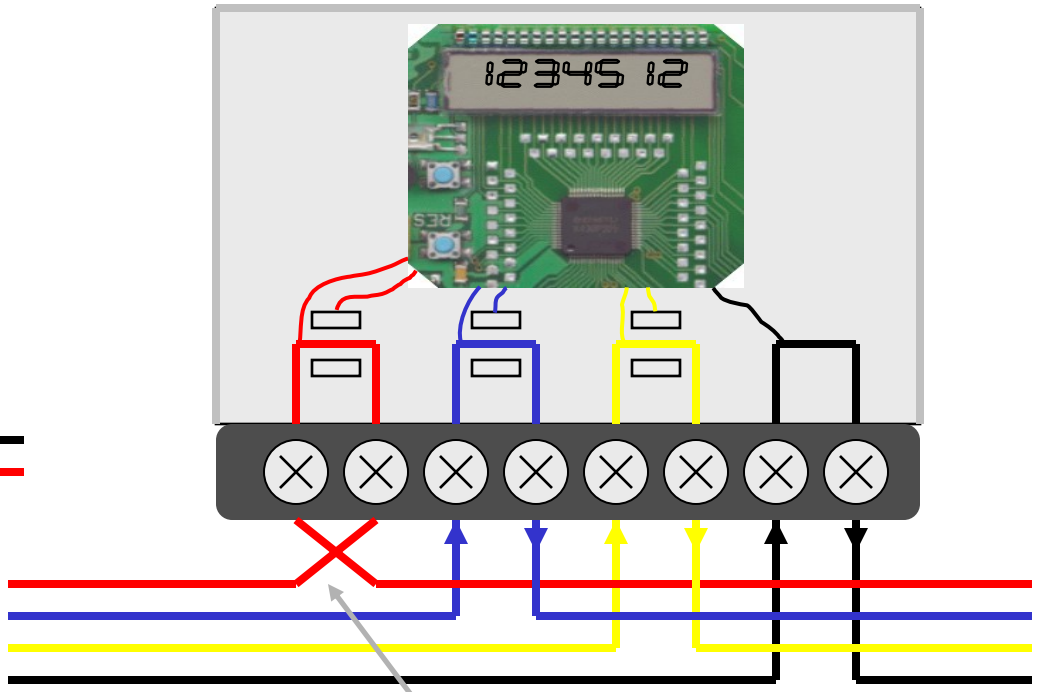
Reverse current tampering cont…

Simple single phase meter



Changes **can't** be left permanently in place, or the meter will read a negative consumption level.

Simple 3 phase meter



Changes **can** be left permanently in place, as the meter will accumulate an average of 1/3rd of the correct consumption level.

Reverse current tampering cont…

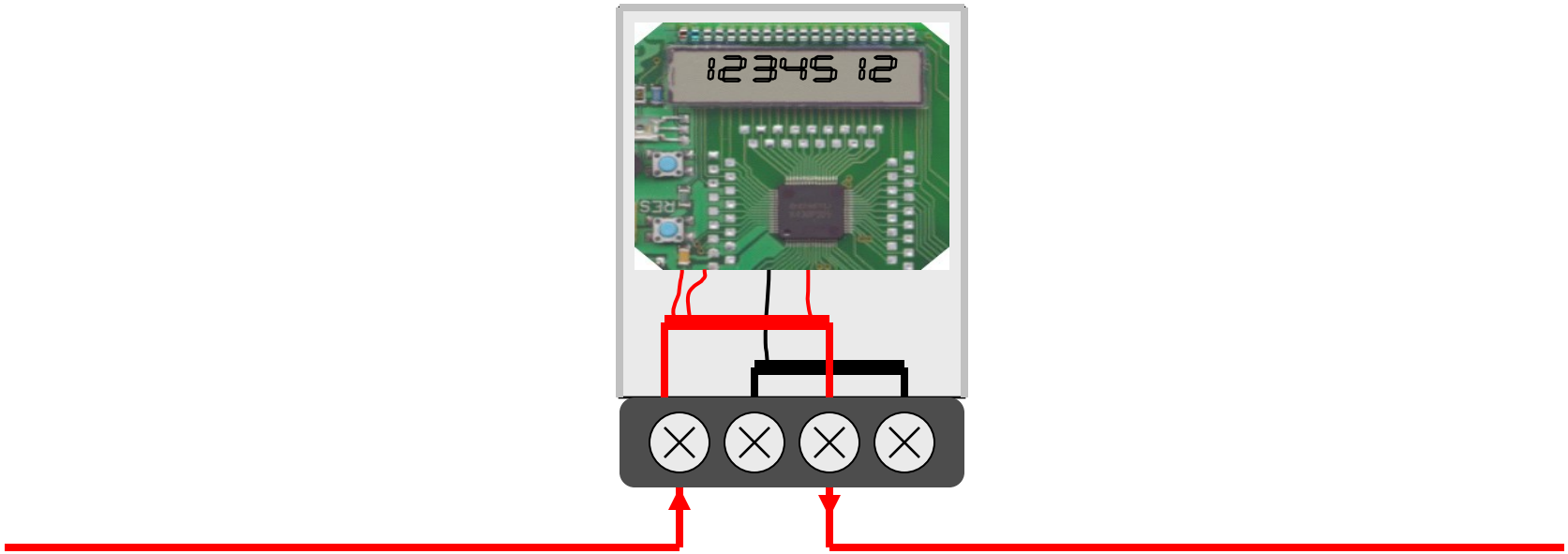
- General strategy is if the absolute measured power is less than zero, in the lead currently being used for measurements, we take special action.
- Care is needed with combinations of tampering.
- Care is needed, so EMI conditions do not cause false detections of reversed current.
  - Persistence checking and careful choice of thresholds may be needed.
- Meters usually have a "Reversed" indicator.
  - Typically an LED.
  - Moving toward the use of LCD segments to lower cost.
- Meters may record the time and duration of periods when reversed current is detected.

Single phase limp mode

- Limp, or live only, mode allows the meter to function in a limited way with one lead completely disconnected.
- A parasitic CT is usually used to extract a little power from the current flowing in the remaining connected lead.
- No voltage signal is available.
  - Measured current is multiplied by the meter's nominal voltage to produce the measured power.
  - No allowance for power factor or exact voltage is possible.
- Typically specified to work with loads greater than 2A.
  - Utilities are interested in lowering the starting current.
  - Some now demand the meter can start a load of 1A.

Single phase limp mode cont…

Simple single phase meter



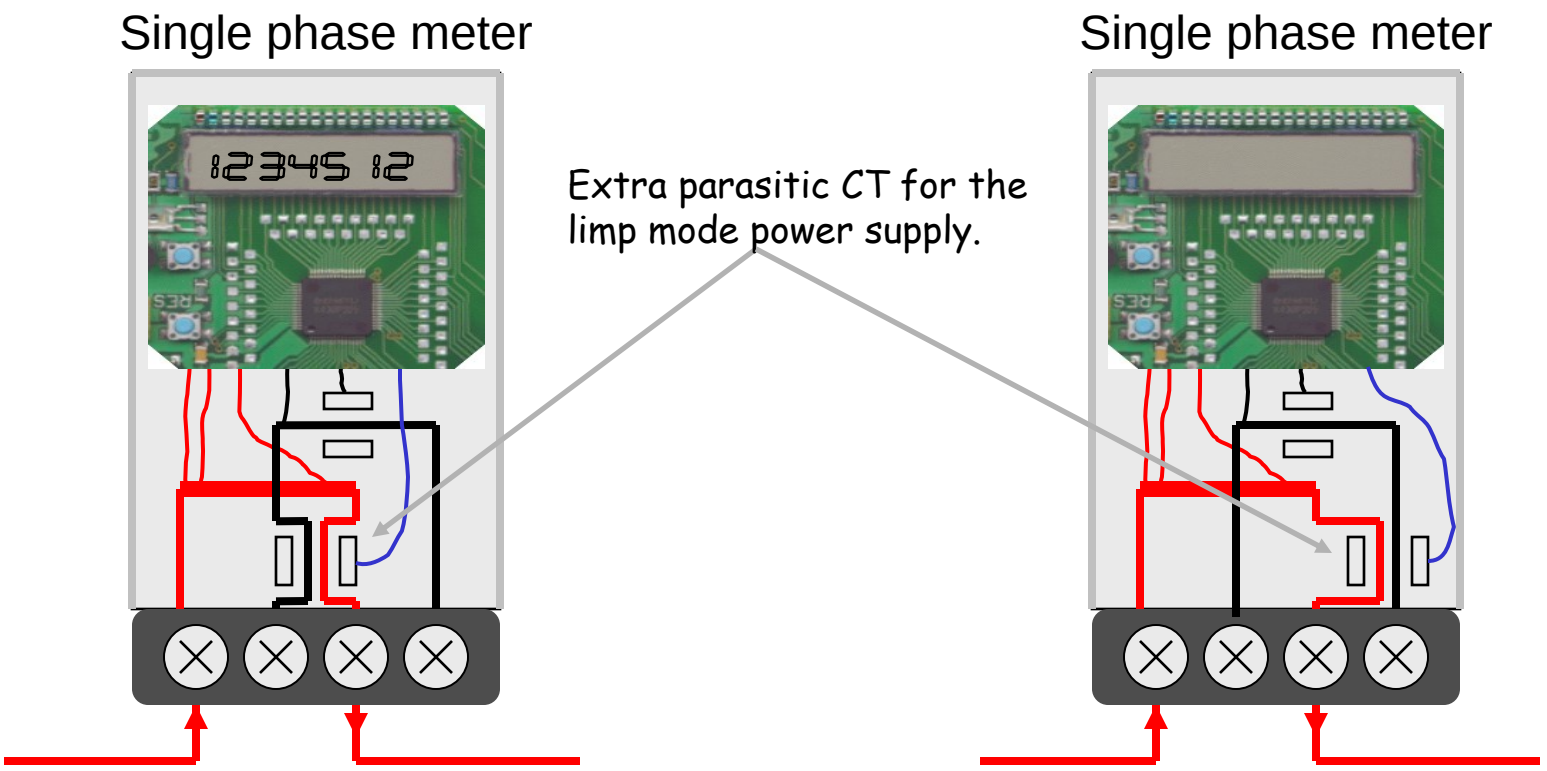
Single phase limp mode cont…

- A CT is added, wrapped around both leads, to generate a little power when current flows.
  - Works whichever lead is disconnected.
  - Only powers the meter when the load current is >1A or >2A.
- Meters usually have two power supplies.
  - A supply driven from the voltage between live and neutral.
    - An RC supply, where isolation not required.
    - A transformer supply where isolation is required (e.g. for an RS485 interface).
  - A CT wrapped around both the live and neutral leads.

Single phase limp mode cont…

- An RC main supply is preferred.
  - Lower cost.
  - Very wide operating range, without excessive dissipation.
  - Has no magnetic components subject to magnetic field saturation tampering.

Single phase limp mode cont…



Currents normally sum in the extra CT.

Currents normally cancel in the extra CT.

Single phase limp mode cont…

- The CT supply needs to drive the meter at the lowest possible current
  - 1A or 2A starting current usually required.
  - A small CT can only generate about 1mA at 3V from a 1A load.
  - Multiple turns of the CT primary lead can increase output, but are clumsy for manufacturing.
  - If several milliamps are supplied at startup, the energy which must be dissipated at maximum load can be high.
  - Current surge conditions (e.g. a >1000A surge under fault conditions, before the breaker trips) must be tolerated.
  - Opposing live and neutral leads reduce normal mode dissipation, but full load and surges must be tolerated in limp mode.
  - Greatly favours an ultra lower power solution, like the MSP430.

Single phase limp mode cont…

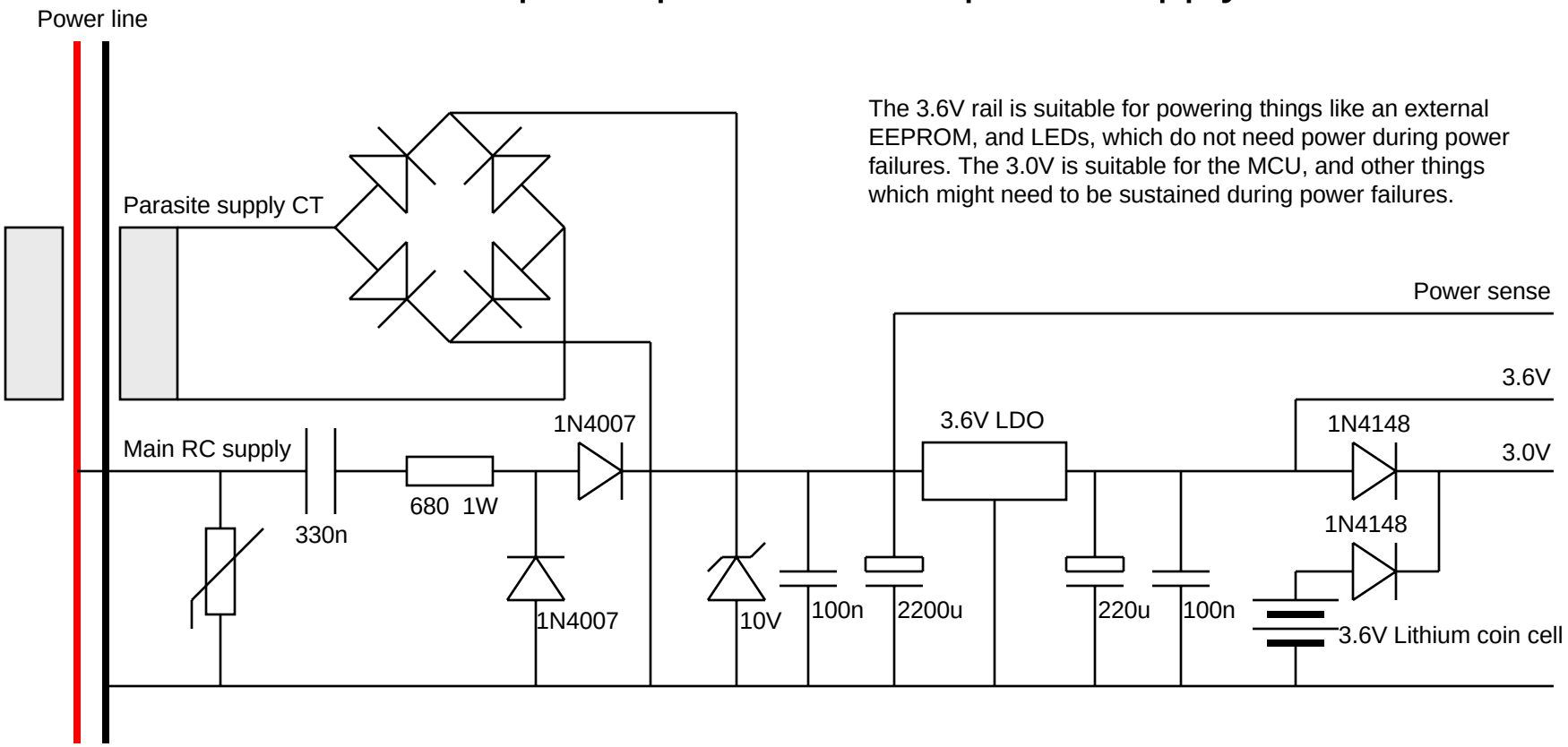
- Power measurement accuracy is not too important in limp mode.
  - Most specifications do not specify the accuracy.
  - High current accuracy without power factor information would be pointless.
  - The estimated voltage may be several percent in error, even in city areas.
  - Reduced sampling can be used, to save power.
- Care is needed to avoid false indications, due to coupling through the parasitic supply CT.
  - Shorting the disconnected terminals can cause a current to flow, which is almost as large as current in the active lead.
  - Need to avoid false reverse current indications.

Single phase limp mode cont.

- Meters usually use the pre-regulator power supply voltage to wake them up when load current flows.
- Meters must behave sensibly when the load current is below the starting current.
  - Before the main electronics starts the power supply will charge up with very small load currents.
  - Once the electronics starts up, too small a load current will cause the power supply voltage to decrease until the main electronics shuts down.
  - This will keep repeating, but should not be allowed to cause flashing indications to the user.
- Measuring current in both leads and the voltage is highly desirable.
  - Monitoring the true voltage permits better meter behaviour.

Single phase limp mode cont.

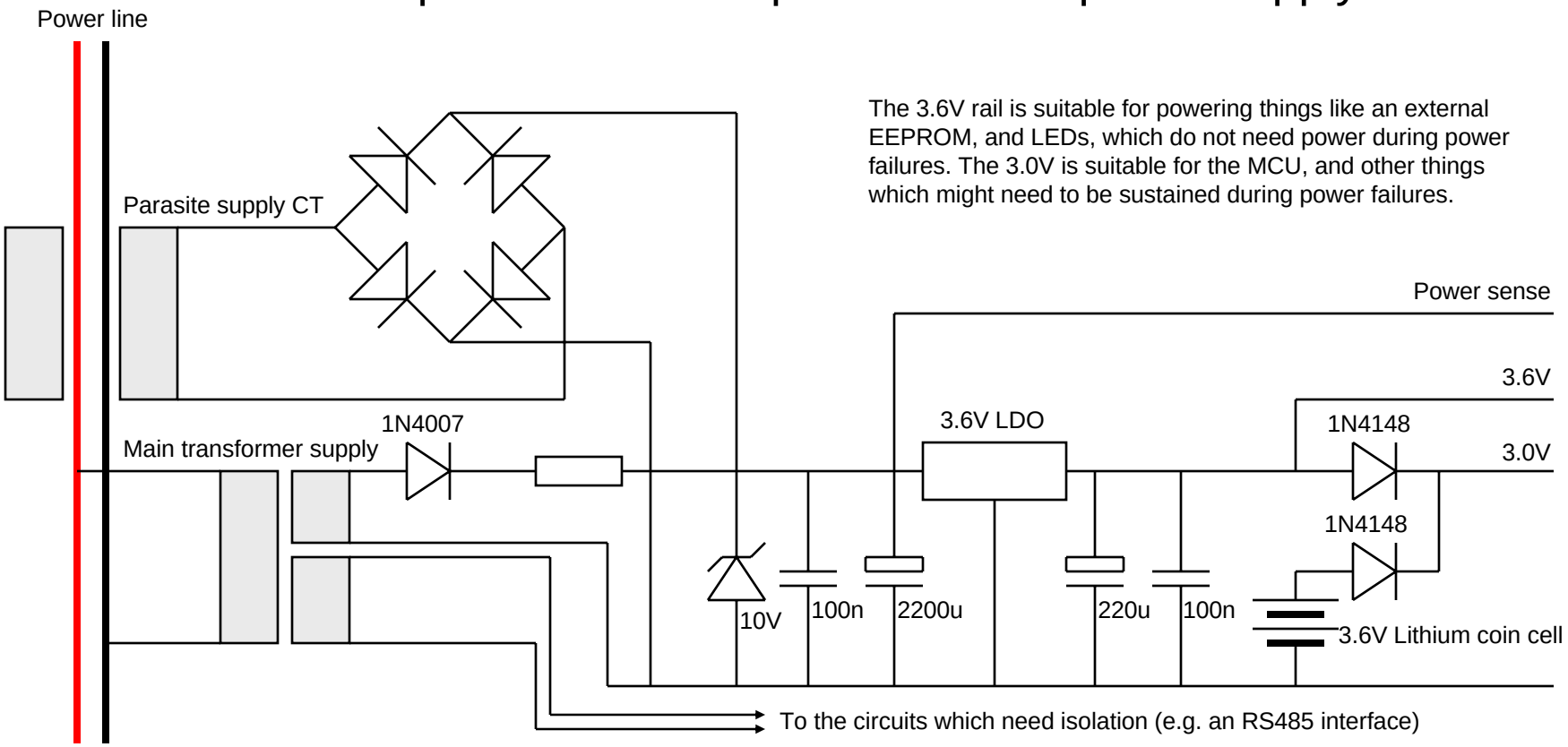
Example limp mode meter power supply



The 3.6V rail is suitable for powering things like an external EEPROM, and LEDs, which do not need power during power failures. The 3.0V is suitable for the MCU, and other things which might need to be sustained during power failures.

Single phase limp mode cont.

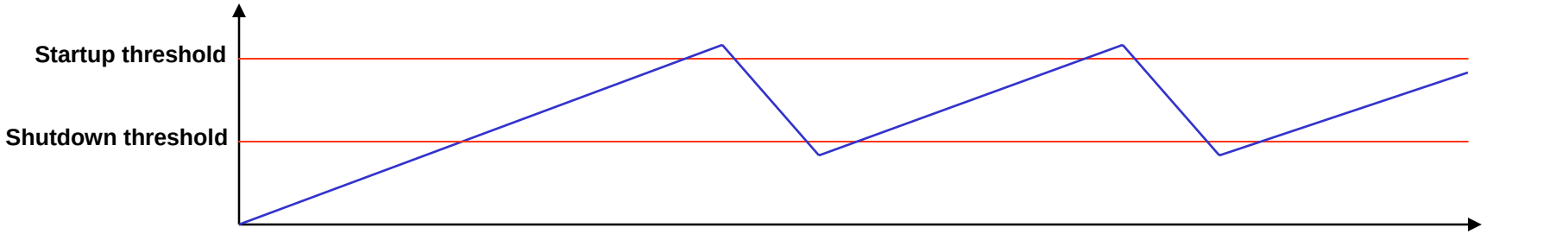
Example isolatable limp mode meter power supply



The 3.6V rail is suitable for powering things like an external EEPROM, and LEDs, which do not need power during power failures. The 3.0V is suitable for the MCU, and other things which might need to be sustained during power failures.

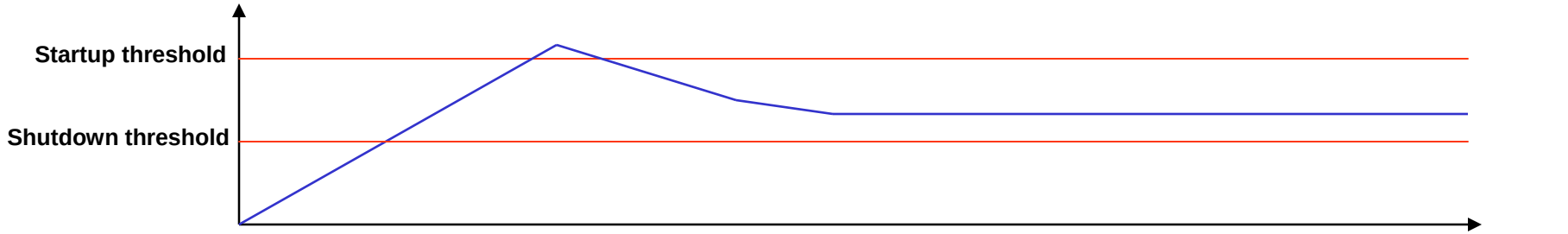
Single phase limp mode cont.

Pre-regulator supply voltage



Small load current startup in limp mode

Pre-regulator supply voltage



Larger load current startup in limp mode

Single phase limp mode cont.

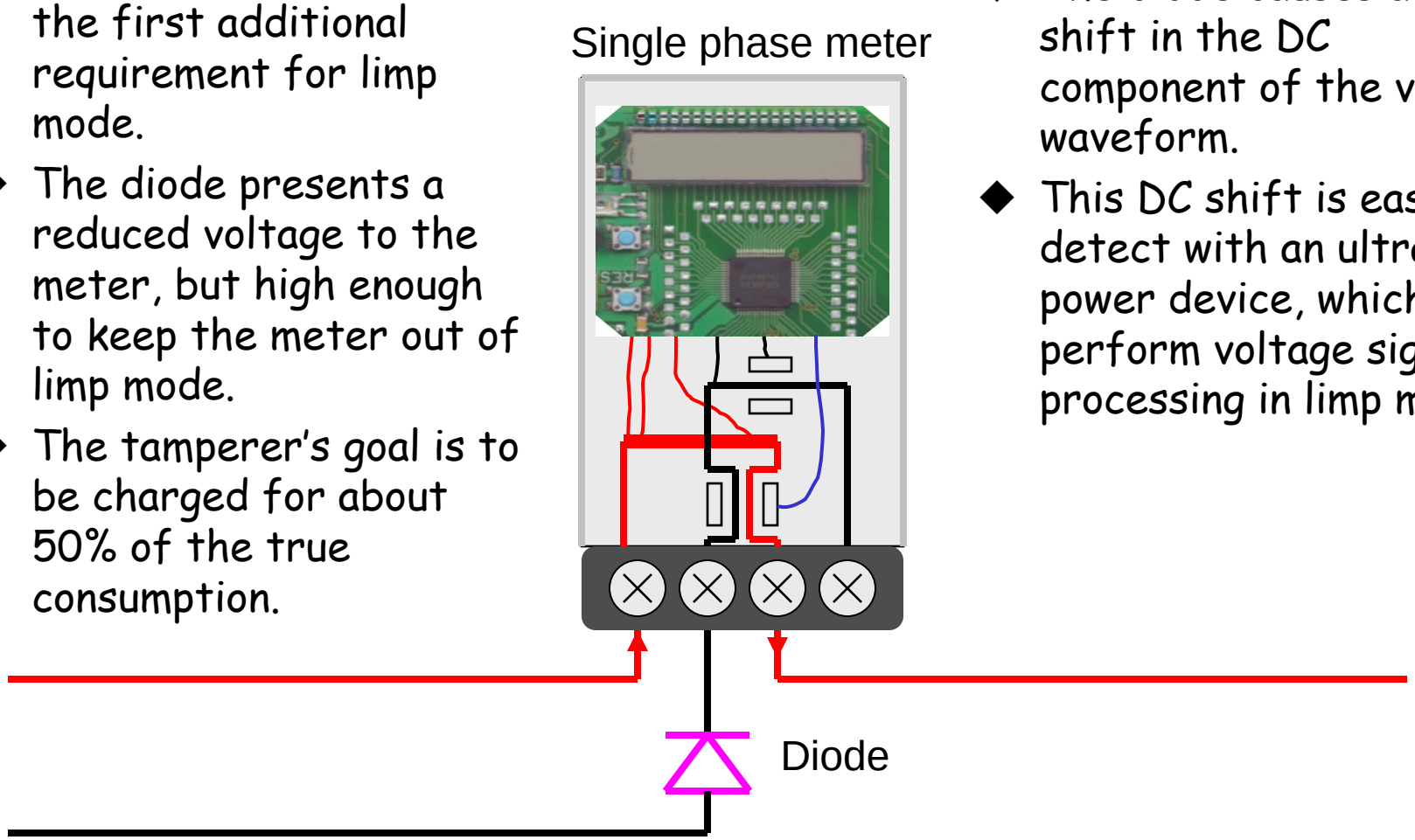
- The meter always wakes up in limp mode.
  - If it woke up in normal operation current consumption would be too high, and the meter could go back to sleep before it has made a proper choice about the right mode.
  - The large supply capacitor is guaranteed to keep the meter running long enough in limp mode, that it can make proper decisions.
- Meters usually have a "Limp" indicator.
  - Typically an LED.
    - High current drain a serious drawback.
  - Moving toward the use of LCD segments to lower cost.
    - Much better power consumption.

Limp mode plus

- First generation limp mode considered only a disconnected lead – i.e. near zero voltage.
- Someone might disconnect one lead, and attach a simple component network
  - Provide enough voltage to avoid triggering limp mode
  - A diode, a resistor, a capacitor, or some combination might be used.
  - Cheap easily available devices, like triac based light dimmers, might be used.
  - They hope to be charged at a reduced rate.
- Need to distinguish a low voltage due to this kind of tampering from a low voltage due to supply conditions (especially in rural areas).

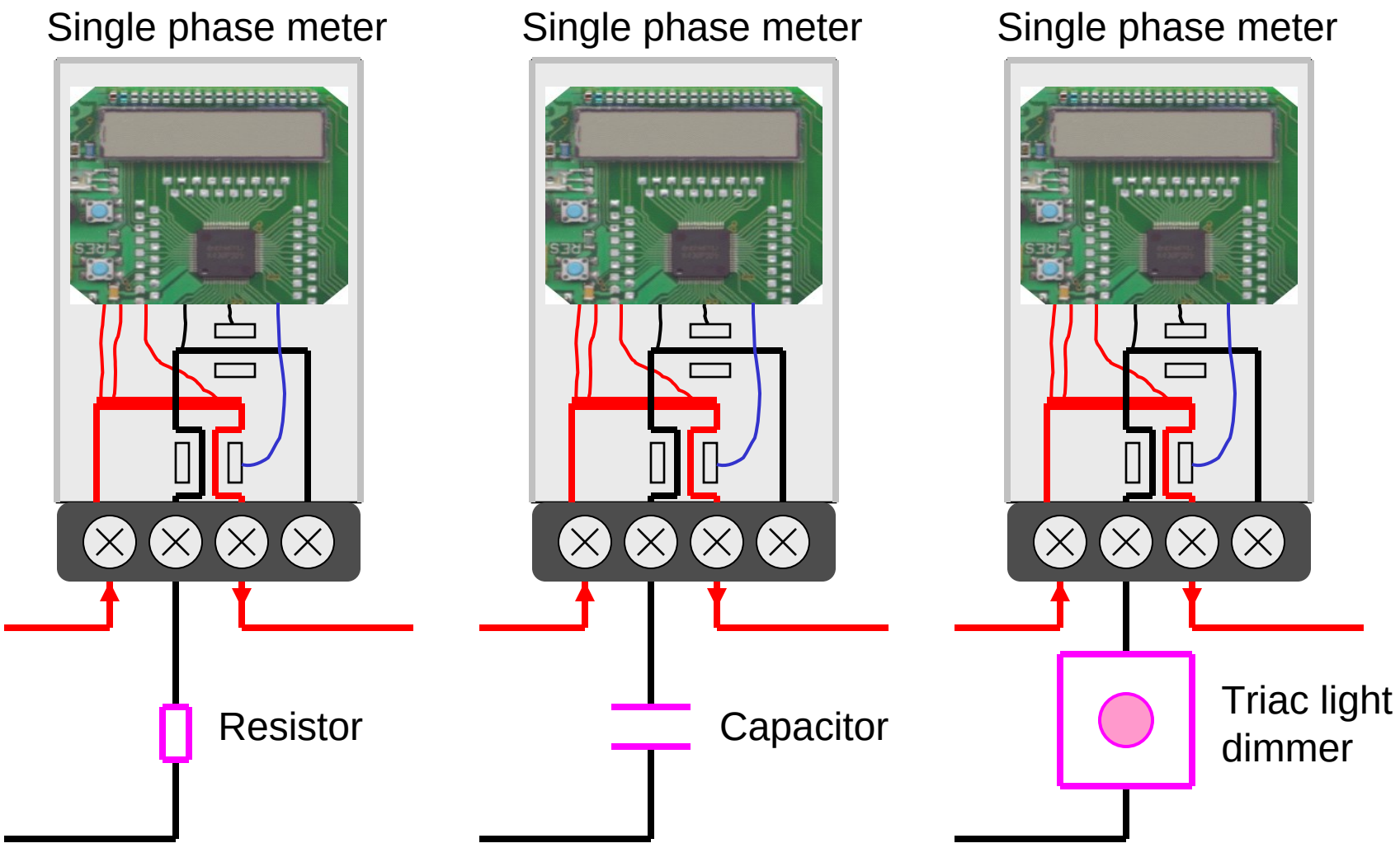
Limp mode plus cont…

- "Diode tolerance" was the first additional requirement for limp mode.
- The diode presents a reduced voltage to the meter, but high enough to keep the meter out of limp mode.
- The tamperer's goal is to be charged for about 50% of the true consumption.



- The diode causes a large shift in the DC component of the voltage waveform.
- This DC shift is easy to detect with an ultra low power device, which can perform voltage signal processing in limp mode.

Limp mode plus cont…



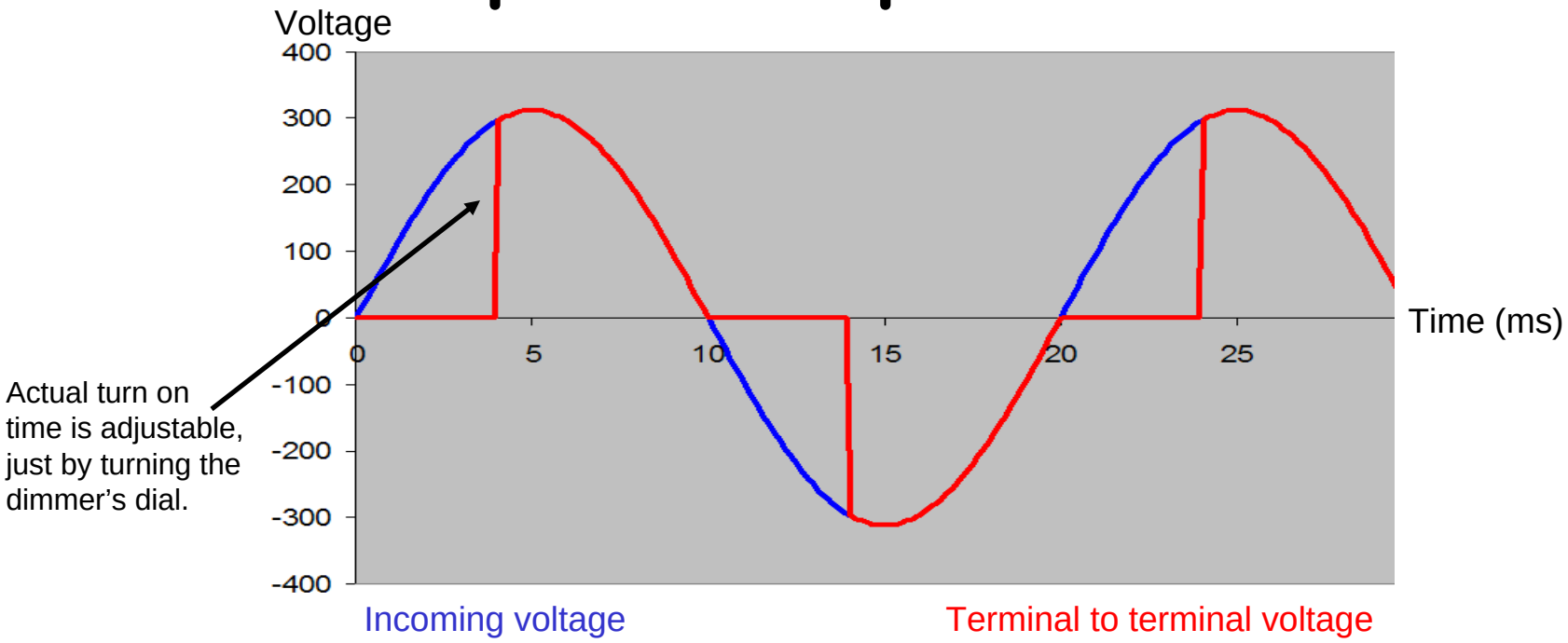
Limp mode plus

- The tamperer would choose a resistor or capacitor to keep the meter out of limp mode, but measuring with a reduced or phase shifted voltage waveform.
- The asymmetry of an RC supply means the apparent DC content of the voltage waveform changes when there is significant impedance in the supply.
- This can reliably identify that the meter is not connected to a proper mains power source.
- The true room temperature DC offset of the analogue circuitry can be stored in flash at calibration time. The normal deviation from that value over time and temperature is small.

Limp mode plus

- Triac based light dimmers are widely available and cheap, so they are a plausible device to use for tampering.
  - Just install and turn the dial for best results.
- With a resistive load (e.g. a light bulb) these dimmers produce a "cut away" voltage waveform.
  - The RMS voltage can be fairly high – keeps the meter out of limp mode.
  - The "cut away" area represent power not measured.
- With an RC supply as the load, they produce something approaching a square wave with a large phase shift.
  - The RMS voltage is higher than normal – keeps the meter out of limp mode.
  - The phase shift greatly reduces the measured power.

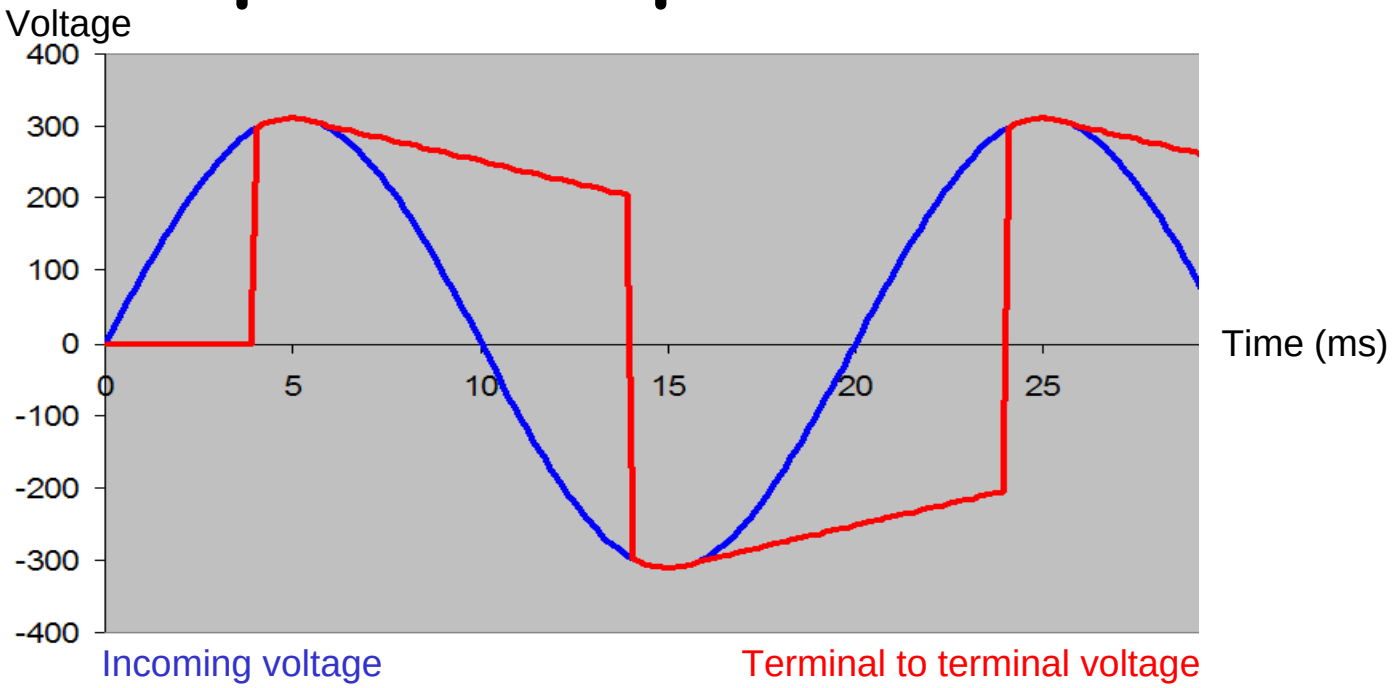
Limp mode plus cont…



Resistive load terminal voltage with a triac light dimmer in circuit.

- Source is 220V, 10A, unity power factor => 2200W.
- Terminal voltage looks heavily shifted to the right – i.e. like a poor power factor.
- The measured power is low because of the apparent power factor.
- Measured result is 183V RMS, 10A, 1532W (70% of the real value).

Limp mode plus cont…



RC supply meter terminal voltage with a triac light dimmer in circuit.

- Source is 220V, 10A, unity power factor => 2200W.
- Terminal voltage looks almost square, and heavily shifted to the right – i.e. like a poor power factor.
- The measured power is low because of the apparent power factor.
- Measured result is 244V RMS, 10A, 1395W (63% of the real value).

Limp mode plus

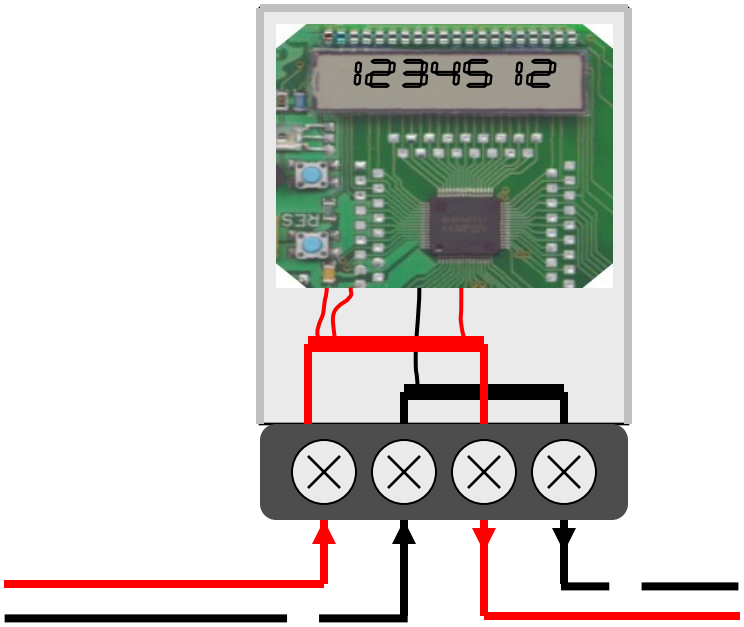
- The voltage waveform looks distorted and has fast edges
  - General distortion not easy to distinguish from a supply with high harmonic content.
  - Fast edges only exist in normal voltage waveforms where there are voltage spikes.
  - Detecting fast edges, and riding over ones which are actually spikes, provides a way to detect the triac dimmer, without a huge computational requirement.
- Requires flexible ultra low power processing
  - Favours processor based solutions, which are easily changed.
  - Favours ultra low power solutions, like the MSP430, which can work within the constraints of the parasitic CT power supply.

3-phase voltage supply tampering

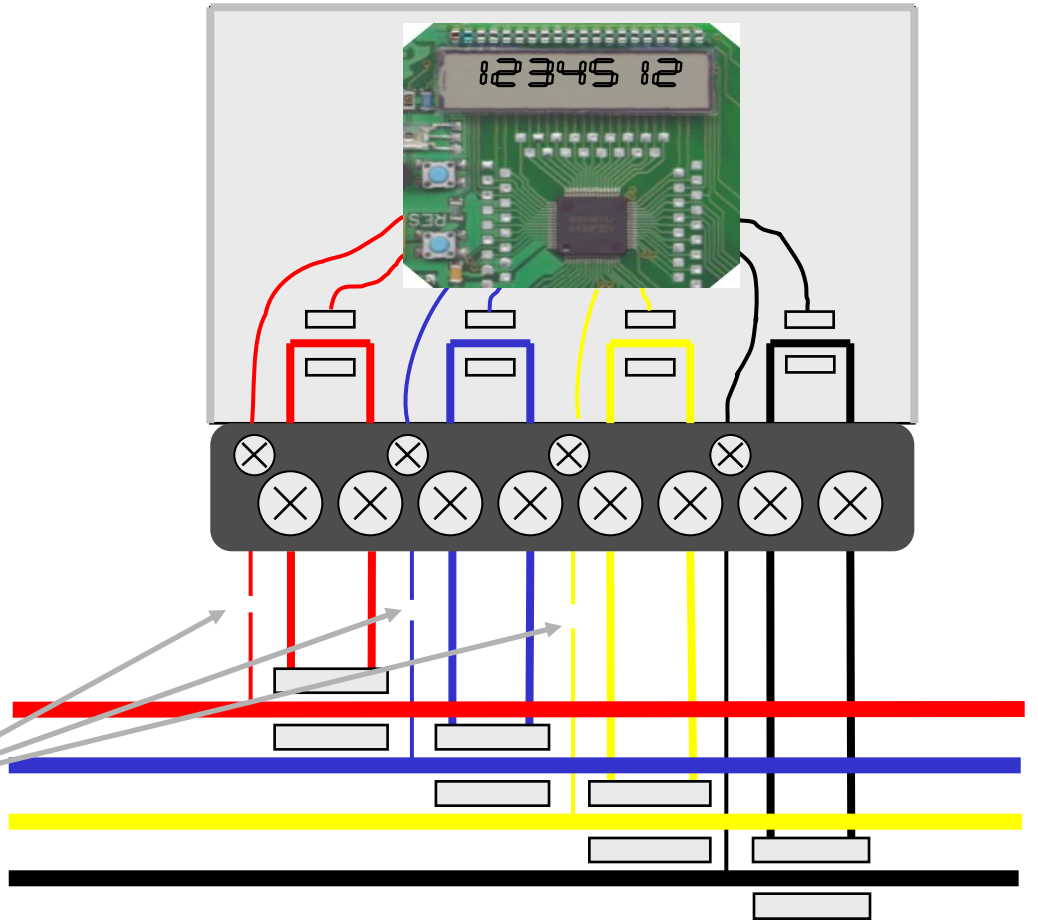
- The 3-phase equivalent to the single phase limp mode.
- Affects meters using external multiplier CTs.
- The tamperer disrupts the voltage signals.
  - The voltage signals can be cut, while leaving the plastic sheath on the wires – can be very hard to see.
  - The large CTs, and their wiring, are left alone, as tampering with them might damage them, and be charged for.

3-phase voltage supply tampering

Simple single phase meter



3 phase meter with external multiplier CTs



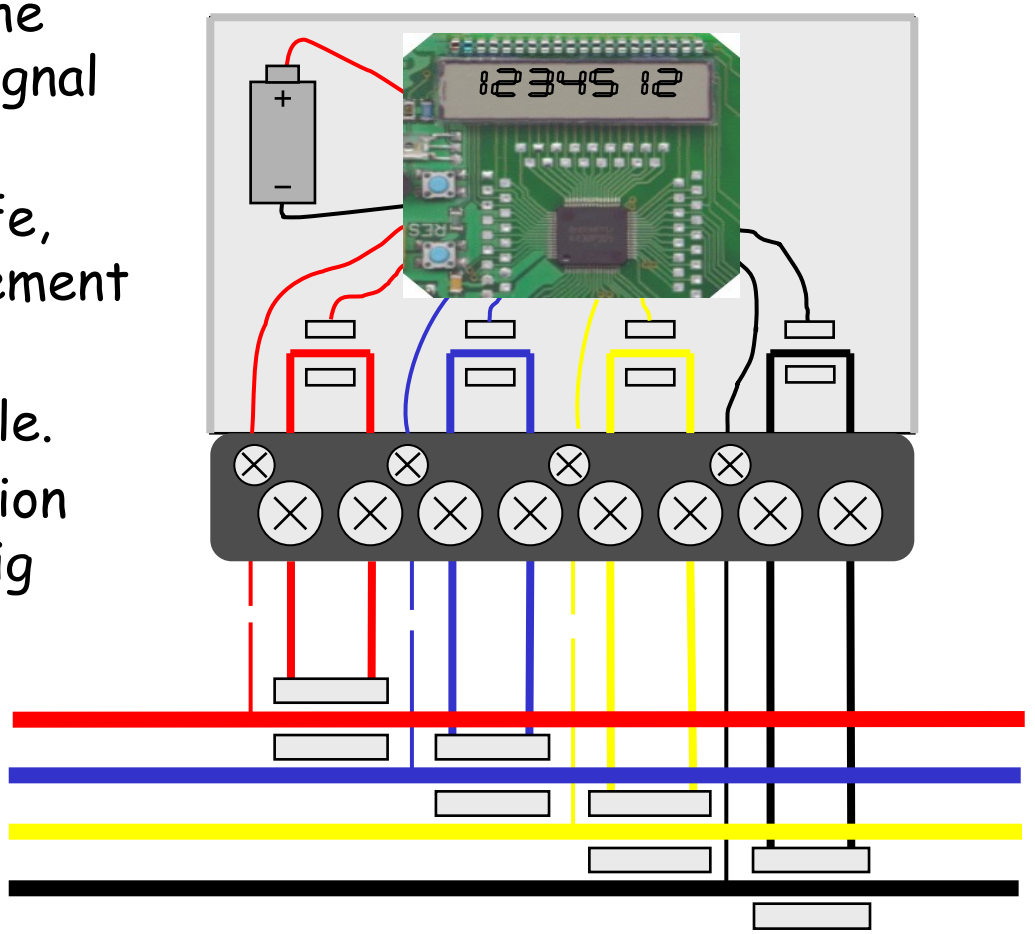
The tamperer cuts the voltage leads, usually leaving the plastic sheath intact.

3-phase voltage supply tampering

One possible response

- Add a battery to power the meter when the voltage signal is cut.
- For reasonable battery life, only intermittent measurement is possible.
- Battery change unavoidable.
- Ultra low power consumption **(e.g. the MSP430)** is a big advantage for maximising battery life.

3 phase meter with external multiplier CTs

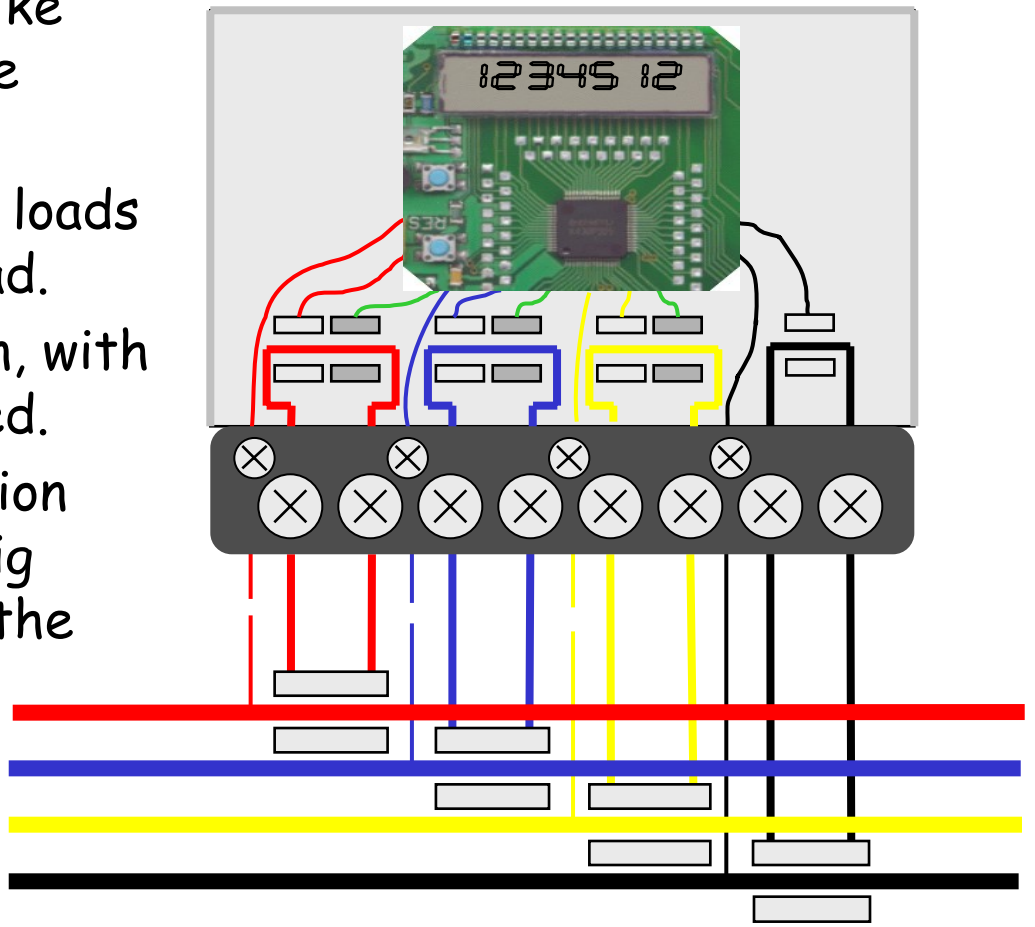


3-phase voltage supply tampering

Alternative response

- Add a CT to each phase, like the single phase limp mode solution.
- The meter can operate at loads above about 2% of full load.
- A "fit and forget" solution, with no battery change required.
- Ultra low power consumption **(e.g. the MSP430)** is a big advantage for minimising the startup current.

3 phase meter with external multiplier CTs



The next step….

- Tolerance requirements seem to be increasing.
  - Higher magnetic tolerance requirements.
  - Tighter balance requirements.
  - Greater physical protection.
  - Enhanced limp mode detection.
- (Guess) AMR allows more complex data to be exchanged, so storing records of tamper detection makes sense.
- Other changes in meters, such as AMR, might be the main area of change from here on.
  - Might permit continuous remote tamper monitoring.