THE COMPLETE POWER LINE COMMUNICATION SYSTEM SOLUTION

Overview

SM6401 is a power line communication transceiver chip. Designed for power line communication network applications, *SM6401* integrates an ultra reliable and robust narrow band power line transceiver with two 32-bit microprocessors (MCU) for both network communication management and user application process. The onboard 32Kbytes Flash making it the most cost effective and versatile PLC product for AMR and HA applications. *SM6401* has been designed with an emphasis on Advanced Metering Infrastructure (AMI) and Automated Meter Reading (AMR) applications where the low cost and the high performance features of *SM6401* are very attractive.

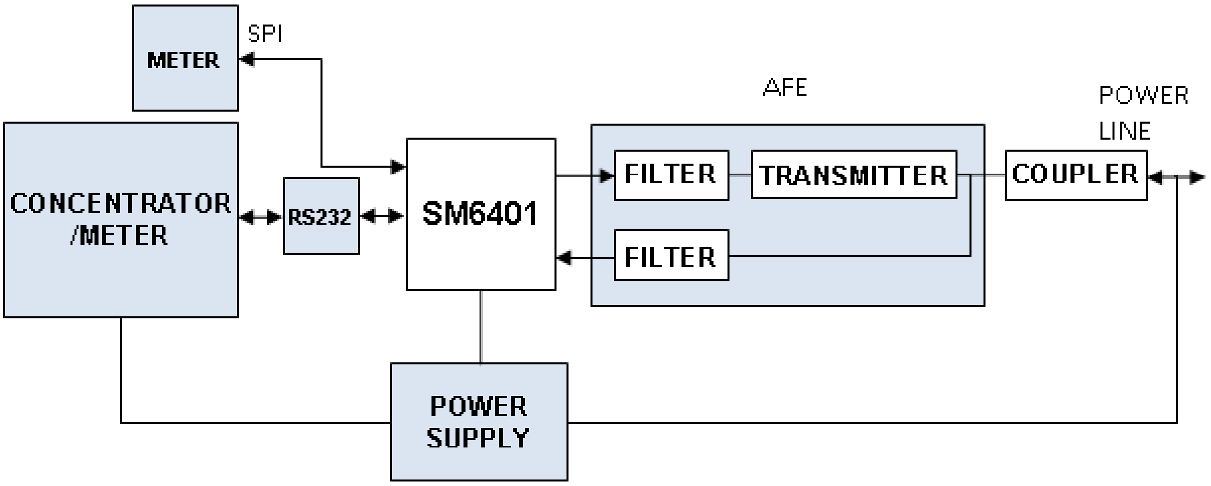
Benefits

- Communicates with existing ANSI / EIA709.1 and ANSI / EIA709.2 devices
- Avoids interference on the power line by having a choice of two communication frequencies on which to transmit and receive data from a list of 8 factory preset frequencies
- User selectable between BPSK modulation for noise immunity and compatibility to ANSI / EIA709.1 and ANSI / EIA709.2 devices and FSK modulation to allow high immunity to the phase distortion
- Approximates the amount of noise on a frequency by direct measurement and the signal strength of received packets
- Embedded user MCU for lower integration costs

Features

- Combines an ANSI / EIA709.1 compliant core with an ANSI / EIA709.2 compliant power line transceiver into a single chip
- Support CENELEC A, B and C band operation
- Medium metrics estimation
- Dual carrier frequencies from a choice of 8 programmable communication frequencies dynamically selectable with programmable baud rate from 5.4kbps to 1kbps
- Triple DES encryption / decryption
- Selectable BPSK and FSK modulation
- Forward Error Correction
- Very high tonal and impulse noise immunity
- A 32-bit EISC processor for EIA709.1 protocol firmware processing
- A dedicated 32-bit EISC processor for user application processing using standard GNU C interface for application code programming
- Receiver sensitivity of -80dBV
- UART and SPI serial interfaces
- Phase detection and mains zero crossing detection
- Up to 21 I/O pins with 5V tolerance
- User RTC / Timers / WatchDog
- 32K byte embedded Flash, 12K byte RAM
- 3.3V supply
- 48-bit unique ID number in each chip

Typical Application Diagram



where AFE is Analogue Front End

Applications

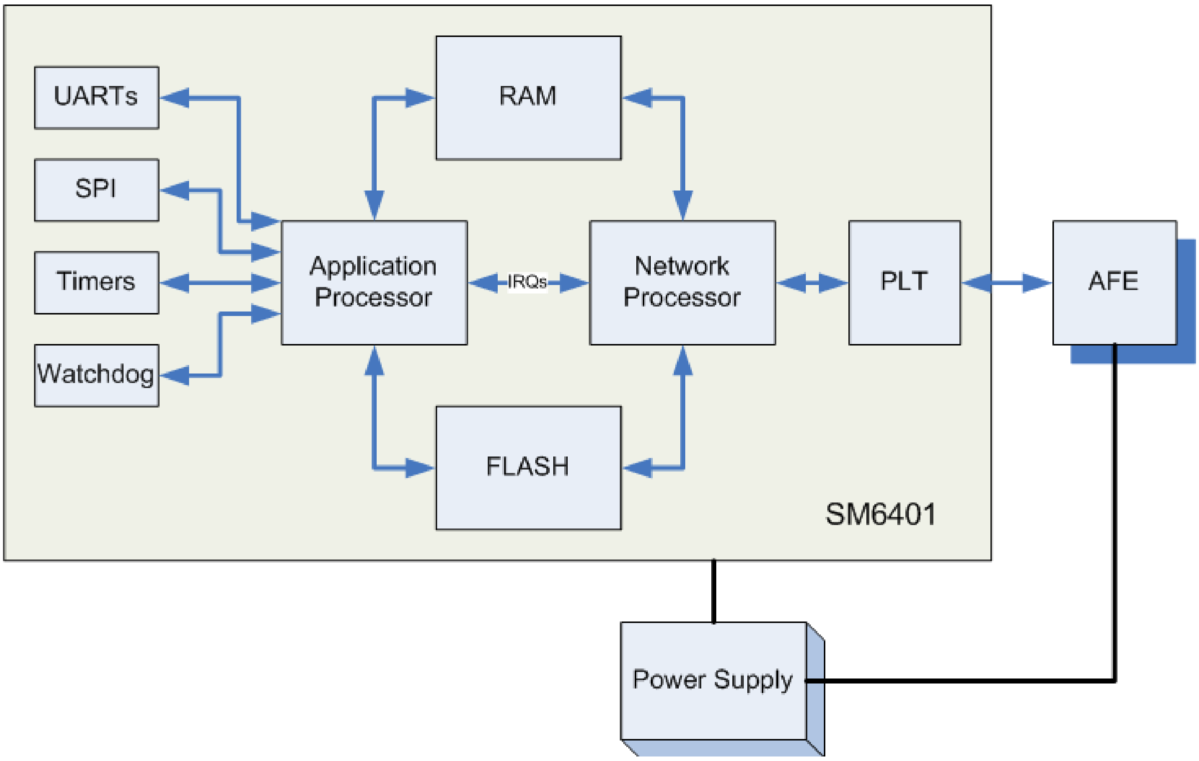
These are a number of applications that the SM6401 is ideally suited for:

- Advanced Metering Infrastructure (AMR)
- Automated Meter Reading (AMI)
- Smart metering and smart grid
- Street lighting control
- Smart energy home area networking
- Home automation (HA)
- Building automation (BA)
- SCADA (Supervisory Control And Data Acquisition)

As can be seen in the diagram above SPI and serial interfaces can be used to interface the SM6401 to meters or concentrators in order to add communications connectivity to existing or new products. The advantage of the SM6401 is that these communications will leverage the existing power line infrastructure for the communications channel. This leads to a cost reduction for a system implementation of one of the above examples compared to other communication solutions.

With the SM6401 containing an embedded MCU for applications, only the SM6401 and the analogue front end has to be added to an existing design for the implementation of power line communications. This also means that devices and products that contain an existing MCU may find that it can be replaced by the SM6401 leading to a cost reduction. This is an advantage for cost sensitive products such as metering.

Block Diagram



where PLT is Power Line Transceiver, AFE is Analogue Front End

Power Line Transceiver

Carrier Frequencies

The *SM6401* programmable carrier frequencies are extremely flexible giving the user control of the communications channel without needing to change oscillator frequencies. Not only can the user choose between eight different carrier frequencies but they also can be controlled dynamically through software, even on a packet-by-packet basis.

This paves the way for dynamic frequency allocation according to the communications medium conditions. The eight frequencies are located within the CENELEC bands. The following table outlines the available carrier frequencies and the corresponding data rates.

Carrier	Frequency	Baud Rate
F0	131.578 kHz	5482 bps
F1	113.636 kHz	4735 bps
F2	104.166 kHz	4340 bps
F3	94.339 kHz	3931 bps
F4	86.206 kHz	3592 bps
F5	79.365 kHz	3307 bps
F6	73.529 kHz	3063 bps
F7	67.567 kHz	2815 bps

Along with the communications medium metric estimation networks can dynamically determine the optimum communications frequencies to use for a particular installation. *SM6401* nodes can communicate with other EIA709.2 based systems when either the F0 or F4 carriers are selected and all other relevant features are correctly configured. Please see EIA709.1/2 compatibility section for details.

Selectable Modulation

The *SM6401* system allows the user to change modulation techniques between FSK and BPSK. This functionality is provided on the secondary channel and can be used as an extra level of redundancy. Abrupt impedance variation can make BPSK demodulation virtually impossible due to the fact that all of the information is encoded into the phase. The phase variation can look like valid data when demodulated. FSK is chosen due to its relatively high immunity to the phase distortion as well as its suitability for use on the power line. FSK and BPSK therefore complement each other by largely overcoming each other's weaknesses by configuring the primary channel to use BPSK and the secondary channel to use FSK. This configuration allows the SM6401 to automatically switch to the alternative modulation scheme on a packet by packet basis.

Dual Receiver Transmitter Mode

The *SM6401* can operate on two different carrier frequencies simultaneously. These two transmission frequencies can be used for a variety of applications. In the case of other EIA709.2 based systems the secondary channel is superfluous and only used when communications on the primary are no longer possible. This could be due to particular devices on the power line jamming communications at the primary carrier frequency. With the dual channel mode enabled the last two retries of acknowledged service messages are sent using the secondary carrier frequency. This enables automatic enabling of the redundant carrier frequency in an attempt to finish the data transmission transaction. All *SM6401* nodes that wish to communicate in this fashion have to be configured for the same carrier frequencies in order to make communications possible. A minimum of two retries must be used in this mode so that the first packet sent will be tried on the primary channel and then the secondary channel will be used. Dual channel mode can also be use in applications were common channel repeating is needed. Parts of a network can be segregated into different frequencies in order to effectively isolate the communication channels. *SM6401* nodes can then be configured to repeat packets across the different carrier frequencies. The two carrier frequencies can be configured as any of the eight frequencies outlined in the carrier frequencies section.

Communication Medium Metric Estimation

Each *SM6401* has the ability to estimate two communications medium metrics. The first metric is an estimate of in-band noise level. Whilst idle a *SM6401* node can acquire a 16-bit value, which approximates the amount of noise that is presented to the node within the transmission frequency. This in band noise metric is the received idle noise level averaged over a period of time. It is recommended that multiple readings are taken and averaged once again due to the large fluctuations of noise commonly seen on power lines. Generally the less noise (e.g. the lower the acquired in band noise metric) the more reliable communications will be. The second metric is an estimate of received signal strength. Each packet received can be interrogated for its estimated signal strength. This is very useful to determine the signal to noise ratio of different nodes on the network. It may be that the noise in a particular band is low but the signal is also attenuated significantly making data transmission unreliable. Network management systems can also interrogate each node for signal to noise ratios to create a database of all transmission path conditions. This produces a deterministic way of finding where repeaters are needed in a difficult environment even if they are dynamic.

EIA / CENELEC Medium Access Protocol

The *SM6401* has selectable medium access protocols to keep it in line with local regulatory bodies. *SM6401* can be configured to use either the CENELEC or EIA709.1 access protocols. When CENELEC mode is selected it is compliant with the Access protocol outlined in the EN 50065-1:2001 standard, sub-clause 5. Maximum theoretical throughput is reduced whilst in this mode.

CENELEC outlines that every power line communications device must monitor the band from 131.5kHz to 133.5kHz and be able to detect the presence of a signal that is asserted for at least 4ms and of at least 86dBµVrms amplitude. A power line signalling device is permitted to transmit if the band-in-use (BIU) shows that the medium has been inactive for at least 85 milliseconds. Each device must then choose a random interval for transmission, and at least seven evenly distributed intervals must be available for random selection.

Error Correction Mode

Devastating noise on the power lines comes in many forms. Noise that is bursting or impulsive in nature can typically have the effect of destroying a whole byte of data. Most power line communication systems are unable to recover from such noise. If the noise is also repetitive in nature then communications may never normally be possible. When error correction mode is enabled a *SM6401* node has the ability to correct for multiple errors that would normally be unrecoverable in most other systems. When in this mode the data throughput rate is lowered by approximately 20%. Error correction can be enabled and disabled through software.

Encryption Mode

SM6401 possesses integrated Triple DES encryption/decryption hardware acceleration. Due to the power line being an open medium any individual has the ability to read transmitted packets. There is even the possibility of intercepting packets, then manipulating data to falsify information. *SM6401*'s strong encryption overcomes the problems of packet sniffing and manipulating data. Although the EIA709.1 protocol claims to have encryption it is not the case. The original message is transmitted “in the clear” when using EIA709.1 Authentication. *SM6401*'s encryption keys are field updateable to allow key rotation once significant amounts of data have been transferred.

Variable BIU Threshold

The CENELEC EN50065-1: 2001 standard, sub-clause 5 specifies that the Band-In-Use threshold level is set at an amplitude of 86dBµVrms. This level may not always be practical in many installations. Many environments contain noise levels that are in excess of this threshold level making reliable medium access impossible. It is for this reason that *SM6401* offers a variable Band-In-Use threshold to accommodate the ambient noise levels of a wide range of installations, with programmable hysteresis.

Mains Synchronization

When the ACSYNC pin is connected in the correct manner a *SM6401* node is able to synchronise to the phase of the AC power. Mains synchronisation can help in overcoming particular sources of noise on the power lines by transmitting at a user defined point of the AC power cycle.

Phase Detection

SM6401 has the ability to detect if two nodes are connected to the same phase. The *SM6401* is able to provide the relative phase angle difference between the two nodes. The ACSYNC pin must be connected as described in the mains synchronisation configuration setting. The node must send a phase detection packet addressed to a remote node, the remote node will respond with the relative phase. This can be used in the field, as often in installations we are unable to ascertain if two power lines are on the same phase. Inter-phase communications are often difficult due to the large amounts of attenuation across phase couplings. During installation it is almost always best to communicate on the same phase.

EIA709.1/2 Interoperability

In their basic mode of operation, *SM6401* nodes are compatible with other EIA709.1/2 based systems.

Advanced features such as error correction and encryption must be turned off in order to enable communications with other EIA709.1 based systems.

To ensure interoperability with EIA709.2 devices *SM6401* must be configured to use BPSK modulation and 132kHz (C-band). For compatibility with some other EIA709.2 derivative devices a carrier frequency of 86kHz (A-band) is also possible.

As *SM6401* incorporates a dual channel transceiver it is possible to configure the primary channel as 132kHz and the secondary channel as 86kHz, or vice versa.

Hardware Modules / Features

In-System Programmable

SM6401 is “in system programmable”; there is a boot-loader in on-chip ROM that facilitates the programming of the on-chip flash memory via an on-chip UART. The ROM loader programs the flash images needed for proper operation. The flash contents may also be updated remotely over the power-line if required.

The system initialisation and boot-loader behaviour is controlled by two pins, *“Boot[1]”* and *“Boot[2]/WEN”*.

These two pins are read when the *SM6401* boots, the state of these pins at reset determine the boot behaviour.

Boot Sequence Control Pins:

Boot[2]	Boot[1]	Boot / Run mode
0	0	*Reserved*
1	0	Program
X	1	Run / Debug

The *“Boot[2]”* pin also functions as the Non-Volatile (NV) operations enable for the System flash,. This pin is continuously polled, any change in the pins state, even after boot, will have effect. The NV operations affected by this pin are the programming and erasing of the system flash.

System Flash Non Volatile Enable:

Boot[2]	Boot[1]	Write Protect Status
0	X	System Flash Erase / Programming **Disabled**
1	X	System Flash Erase / Programming **Enabled**

Full Duplex UART

There are two full duplex universal asynchronous receiver/transmitters (UART) in the *SM6401*. They support baud rates from 1.25 mega baud down to 300 baud.

The frame format is:

- 0 / 1 start bits,
- 7 ~ 10 data bits,
- Odd / Even / No parity,
- 0 / 1 / 2 stop bits.

Each UART can generate a receive buffer full or transmit buffer empty interrupt.

With start and stop bits disabled, the serial port can act as a bit shifter.

There are individually configurable hardware handshake pins with programmable polarity.

Hardware Timers

There are four 32-bit count-down timers; they can each generate an interrupt. The timers have a 50 ns time base.

There are pre–scale settings for modifying the default time base. The pre scale settings can be from a one ms pre-scalar, the 32kHz timer, or the UART baud rate timer.

The timers can be set up to count interrupts from an I/O Port, or from the other timer. The timers can be set to cyclic mode, where they automatically reload, making them useful for periodic timing functions.

GPIO

All user I/O pins are multifunction. Each I/O can be used as a general purpose input/ output pin, each pin can alternatively be used as a special function these include:

- UART
- SPI

The pins are organised into ports that can be manipulated on a byte level.

There is a bank of interrupt pins.

All of the GPIO ports are 3.3V, 5V tolerant and bi-directional.

SPI Input/Output

SM6401 includes a full Master/Slave SPI module with following features:

- Master or slave mode
- Multi-master bus contention detection and interrupt
- Four transfer protocols available with selectable clock polarity and clock phase

- Variable length of transfer word up to 16 bits
- Compatible with SPI (a trademark of Motorola Semiconductor) and Microwire / Plus (a trademark of National Semiconductor)
- Bit rates generated in Master mode: ÷2 down to ÷256 of System clock
- Bit rates supported in Slave mode: SCK = System clock ÷4

Break Point Register

There are 3 comparator breakpoints useful for debugging. They can be set to generate breakpoints on:

- instructions
- addresses
- data

These breakpoints can be chained to generate an interrupt only if two or more comparators match their values.

These registers are used by the GNU debugger (GDB).

Watch Dog Timer

This timer can have a period between 1ms and 2 sec. It can be configured to generate an interrupt or to reset the *SM6401*.

Interrupt Controller

All interrupts may be blocked, cleared or set in software. There are interrupts for:

- Illegal bus transactions
- A watchdog IRQ
- Network events
- An IRQ for I/O events (8 pins can generate irq events)
- An IRQ for UART events (rx and tx buffers)
- An SPI IRQ
- Separate Timer IRQs

The MCU can be put into a halt mode, where it will stay idle until an interrupt is generated, this reduces power consumption.

Contact Information

For more information regarding the *SM6401* chips including technical data sheets, application notes, sample enquiries, demonstration modules, pricing and ordering please contact:

Semitech Semiconductor Pte Ltd

www.semitechsemi.com

sales@semitechsemi.com

Revision (110)

Version	Description	Date
0.1	Draft	26/07/2010