Secantec, Inc.

EXECUTIVE SUMMARY

Overview - The Quick Pitch

Secantec, Inc. is the sole provider of Forward Error Correction IP. It solves the most complex mathematical problems in silicon, making communication, networking, storage, and chip-to-chip data transfers error-free and fast without disrupting the chip functions.

The Problem

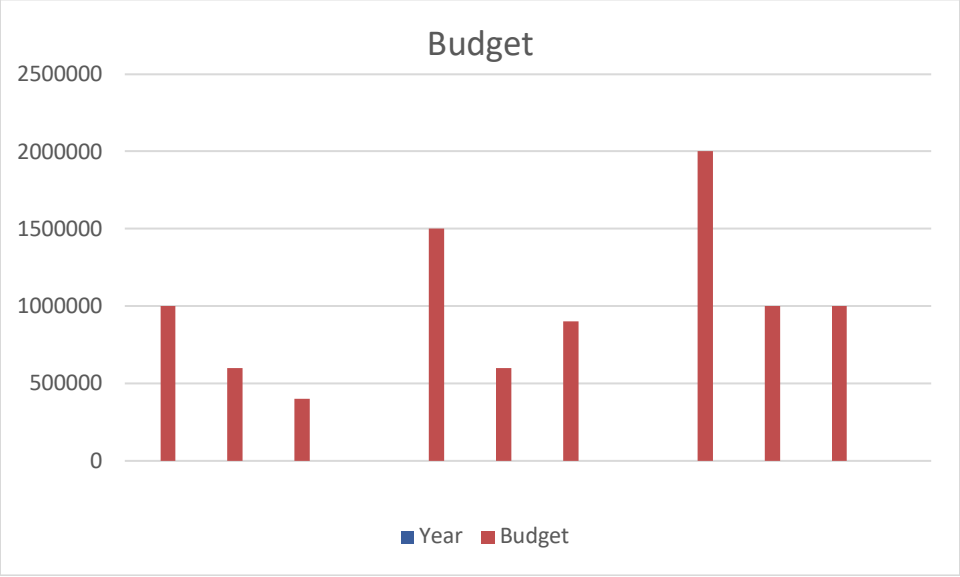
- During data transfers over the air in 5G, or network over the wire, or in the data drives, data may get corrupted due to interference or voltage and temperature fluctuations.
- This is overcome by adding additional logic and parity bits for error correction.
- The problem is severe in 5G, networking, and chip-to-chip communications, as packet retransmission causes higher latency and lower throughput.
- The disk repairs generate significant network traffic, and there is a necessity to keep the overall storage to a minimum.
- Current solutions have high latency and are slow; Secantec's advanced mathematical knowledge makes the IP unique and efficient. Competitors are (1) (2).

The Solution

Secantec has solved the problem using advanced knowledge of Galois Fields Arithmetic and decimal arithmetic. Secantec has expertise in digital design and verification which has been used to develop an entire library of FEC codes for any application. The complex solution has been scripted in Perl to generate code for any requirement.

Highlights

The LDPC Codes are very efficient and can have many applications, including 5G Wimax DVB-S2, 802.11n, etc. This also applies to BCH and RS Codes used in SSD drive data protection and networking data error correction over the wire. There are immense applications for these solutions.



Initial Projected Revenue

Keys to Success

The essential steps for the business are to approach Fortune-10 companies and display the features and advantages of the FEC IP codes. These IPs are necessary for their products and how they can benefit their customers using this intellectual property.
There is a need to raise capital to get the marketing team together and partner with EDA tool vendors.
There should be a sale within a year, as the IP is ready but needs to be rolled out to the proper end customer.

Financial Highlights

$1,500,000 is required for the company to run for a year. The marketing team is responsible for handing over all the IPs to the customers to integrate into their products. Every customer will have their own needs, and as IPs are configurable, this should be easy to generate. If proper customers are targeted, the repayment can be within a year and a half.

Product Highlights

Error-correcting Codes

Error Correction and detection for data in Silicon using BCH Code and Reed Solomon Code, with efficient implementation in RTL for low power and high frequency of operation. There could be an Erasure Correction for disk drive failure in a cluster of disks. The data can be reconstructed for Communication based on an LDPC encoder/decoder. The LDPC has different code block sizes, which can be used for other applications. Hamming code ECC, which is programmable for various data widths.

Errors in Communication, Networking, wear and tear due to continuous use of devices like NAND Flash and b, burst transmission errors on SERDES lines. There can be BCH Error Correction, RS Error Correction, and Fire-Code Error Correction for these requirements in Silicon Devices. These implementations are absolute time-time and correct errors and detect if the block has more than the maximum number of errors allowed. The RTL implementation also adjusts the number of Errors Correctable so that these values can be programmed according to the application requirements. There are also requirements where there are disk drive failures in a cluster of disks; this can also be reconstructed using a Reed Solomon Erasure Correcting Algorithm. The Symbol width can be selected based on the application. The symbol width can be broken into two so that there could be a sub-cluster within a giant cluster which will limit the number of reads on drive failure. When there is a write-on one drive, only the parity can be updated with a read/modify write to the parity drive, and all other drives remain idle. An LDPC encoder/decoder can be used to correct highly efficient errors. The LDPC decoder is iterative decoding, so it consumes time, but the RTL implementation is highly optimized to make the iteration time to a minimum of 4 clocks. The Hamming Code ECC can correct one error and detect up to 2 errors for a given data width. It can be split into smaller parts to increase the accuracy of data to generate Hamming ECC parity bits, but it has a drawback of high overhead bit. This problem can be solved by switching to BCH Code which can handle large data width. The implementation is possible up to 64*1024 data widths but can also go beyond this limit.

There are several types of failures in Silicon systems.

1. Dynamic Errors in Silicon that go undetected due to Process, Voltage, and Temperature variations
2. Memories used in Silicon have more PVT issues while accessing data at high rates.
3. Silicon Devices like NAND Flash introduces more and more errors as the age of device due to wear and tear of continuous use.
4. Communications introduce channel errors due to interference from the surrounding environment.
5. Packet transfers in networking have errors due to interference from unwanted noise.
6. SERDES communication introduces burst errors while sending data point to point.
7. Disk drives failures in a cluster of disks. The clusters can be one big cluster consisting of sub-clusters; this is done to reduce the traffic during the reconstruction of a failed disk.
8. CRC is used to check data integrity after errors are corrected.
9. Scramblers are used to make data pseudo-random to avoid a continuous burst of bit 1 or bit 0

The Project consists of

1. BCH Code RTL implementation, the length of the code block is programmable
   - lengths of code blocks are 7, 15, 31, 63, 127, 255, 511, 1023, …. 64*1024-1,
   - Error correction capability
     - Programmable on the decoder side
     - Need separate encoders for each maximum number of errors correction capability
   - Can process 1 code block per clock
     - RTL implementation is a barrel shifter with processing at every shift
   - Different implementations for different Code blocks
   - The total number of bits in the Code block can be shortened by making the un-needed bits 0
   - The Same implementation can be used if the maximum code lengths for two different codes are the same by different programming values to the RTL.
   - RTL consists of the encoder; on the decoder side, it has a syndrome calculator, BerlekAmp Massey circuitry, and Chien Search
2. Reed Solomon Error Correcting Code implementation
   - lengths of code blocks are 7, 15, 31, 63, 127, 255, 511, 1023, …. 64*1024-1,
   - The corresponding symbol size is 3,4,5,6,7, 8,9, 10,.16, …
   - Error correction capability
     - Programmable on the decoder side
     - Programmable on encode side
   - Can process 1 code block per clock
     - RTL implementation is a barrel shifter with processing at every shift
   - Different implementations for different Code blocks
   - The total number of symbols in the Code block can be shortened by making the unneeded symbols 0
   - The Same implementation can be used if the maximum code lengths for two different codes are the same by different programming values to the RTL.
   - RTL consists of the encoder; on the decoder side, it has a syndrome calculator, BerlekAmp Massey circuitry, and Chien Search and Forney circuitry.
3. Reed Solomon Erasure Code implementation
   - Implementation differs for some blocks from Reed Solomon Error Correcting Code RTL
   - Blocks like Encoder, Syndrome calculator, and Chien Search are the same
   - Blocks of Berlekamp Massy, Forney Calculator differ
   - Same properties for RS ECC apply to the Erasure Code RTL
4. Burst Errors: FireCode FEC
   - The FireCode FEC searches burst errors by calculating 3 CRC width values, e.g., 32, 21,11, and, based on the results, points out if there is an 11-bit burst error in an incoming data stream.
   - The length of the data stream in networking is 2112 for this code but can be variable based on the application.
   - The 3 CRC widths of 32 and 21,11 can differ based on different applications. In that case, only the summation of the last two has to be equal to the first one, and the product of the polynomials for the previous two widths has to be similar to the polynomial of the first CRC width.
5. Hamming Code parity generator
   - The RTL can be generated for any incoming data length.
   - RTL consists of an encoder and decoder.
   - Encoder generated parity bits; the number of parity bits depends on incoming data bits
   - Decoder has 2-bit error detection and 1-bit error correction
   - Encoder and Decoder are asynchronous or are pipelined for getting 1 data length per clock throughput at high frequency
6. LDPC Encoder/Decoder
   - The LDPC Encoder selects certain bits of incoming data, XOR them, and calculates output parity bits
   - The LDPC decoder iteratively corrects bits based on party bits received till the hamming distance is 0
   - There is a different implementation for different parity check matrices. The parity check matrix generated *.alist files, which are processed to generate the RTL code for the encoder and decoder.
   - The Encoder is asynchronous
   - The Decoder can do one iteration in 5 clocks.
7. LDPC q-ary Code
   - The FFT is performed in LDPC q-ary operation
   - The LDPC operates on the Galois field of 3,4,5,6,7,8,9. Either of this degree
   - Work In Progress

8. Polar Codes
   - Based on binary nodes
   - RTL implementation of Encoder is ready based on 5g standards
   - Decoder Work in Progress.
9. Reed-Mullerler: encoder/decoder
   - Work In Progress
10. Locally Reparable Code for RAID in Data Center
   - Work In Progress
11. GCM Mode for AES
   - IP available with AES Encryption and Decryption