**SHA2 Overview**

**General Overview:**

The sha 2 block is a top level design of 3 sha 2 algorithms the sha 256, 284, and 512. These blocks currently consist of a VHDL ip top level and a Verilog Core. Below is information about how the block functions and basic idea of the structure of the block.

**Diagram

Description automatically generated**

My top level plan for the sha2 algorithms is as follows.

CLK and RST will drive the block.

Data will be read in windows of 1024 bits. This will be stored in the data in register that is only available before sending the go signal. This is to prevent starting an operation before another operation completes.

Function Bits will be available to write to before sending the go signal. To select SHA 256 you will need to select 00, SHA 384 select 01, and SHA 512 select 10.

This is to protect the integrity of the operation.

Next, the bus will need to send the go signal to start an operation from the controller. The controller will then send a logic ‘1’ signal to the Go Decoder which will use the function\_bits register to start the correct function.

When the function completes, the data will be stored in a 512 bit register that is enabled by the function done signal.