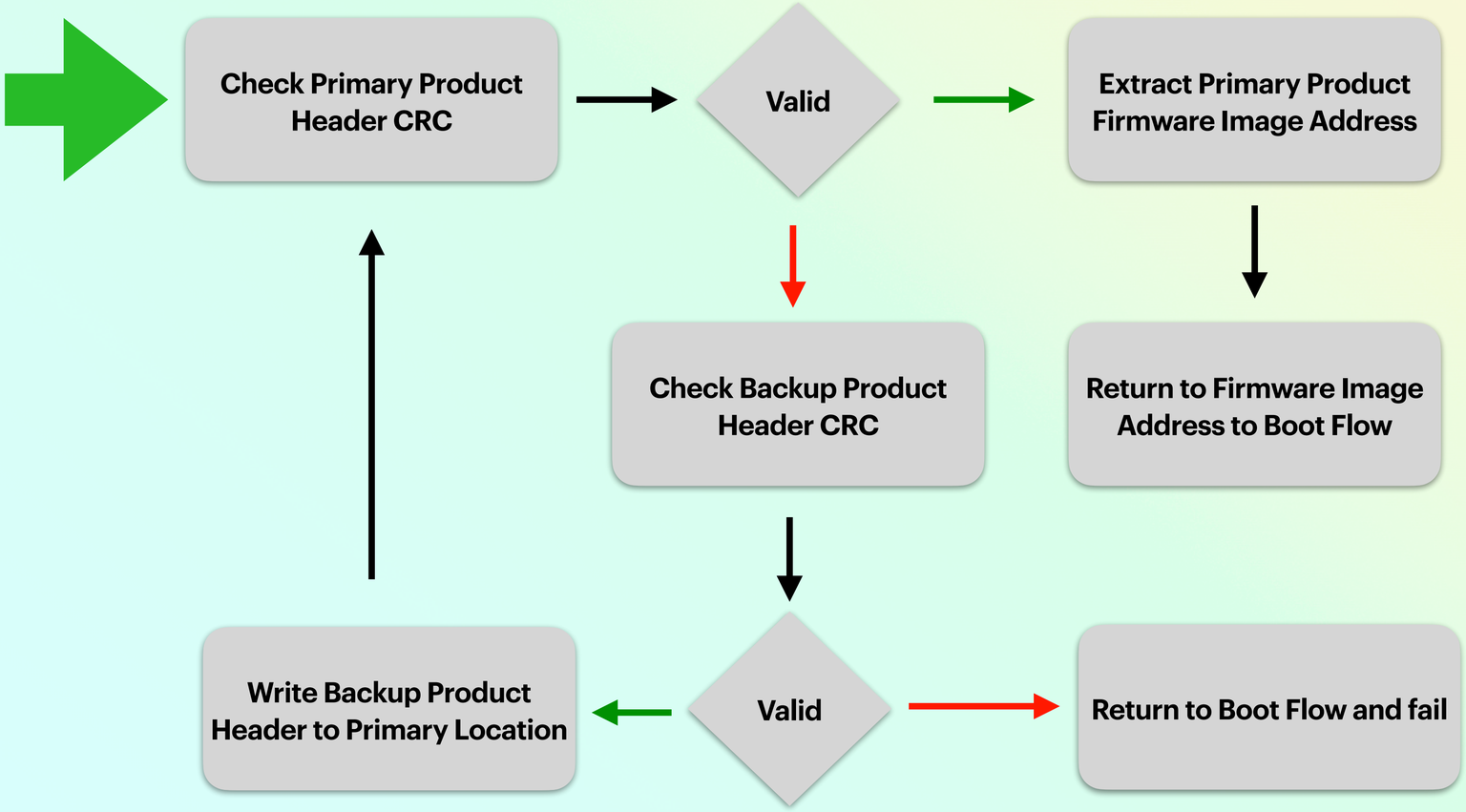
PRODUCT HEADER VALIDATION



Seems ok.

PRODUCT HEADER ~~VALIDATION~~

Nope.

```
void __fastcall QSPI_Read_Product_Headers(struct_configuration_script_ptr *configuration_script_ptr, char *img_offset)
{
  char backup_product_header_buff[258]; // <----- FIXED BUFFER
  __int16 flash_cfg_len; // 2-byte size
  char product_header_id[4];
  unsigned __int16 product_header_length; // 2-byte size
  char is_valid; //
```

backup_product_header_buff[258] - fixed length value

product_header_length - user controlled 2-byte value in the Product Header (Length of Flash Config Section)

```
// read the entire backup header, including the stored CRC at the end
QSPI_Get_Read_Result(backup_product_header_buff, product_header_length + 2);
```

This one was trying its very best to be useful

```
product_header_length = flash_cfg_len + 0x16;
```