Mosaic Industries

Finding Stack Overflows Using C

APPLICATION NOTE
MI-AN-042

Summary

The following shows how to find stack overflows using C.

Description

To determine if the stack has overflowed while using C, we can perform the following to find out how big the stack has gotten. This is for the default task only.

After the code has been downloaded, the stack can be filled with zeros. By looking at the stack after the code has run, it can be seen how big the stack gets.

The default stack starts at 0x8800 and is 512 bytes long. We will start filling the stack at 0x8824 by using the following commands.

```
HEX
8824 0 2CC ERASE
```

To view the stack after the program has run and maybe even crashed, we type in the following.

```
8824 0 2DC DUMP
```

By inspecting the dump, we can see where the stack has been. If there are no 00's left in the dump, then the stack has grown too big.

To change the stack, we can type in the following commands to move the stack to the top of memory. These commands must be typed interactively after the code has been downloaded. This will give the stack and the variables a total of 12K to share.

```
HEX
ADFF R0!
RP!
/ execute main here
```

The information provided herein is believed to be reliable; however, Mosaic Industries assumes no responsibility for inaccuracies or omissions. Mosaic Industries assumes no responsibility for the use of this information and all use of such information shall be entirely at the user's own risk.