MSPM0

Selecting Security Level 1

1/19/2024

MSP Applications, Dennis Lehman

Texas Instruments

Level 1 Features

1.4.2.1.2 SWD Security Level 1

SWD security level 1 allows for a customized security configuration. The physical debug port (SW-DP) is left enabled, and each function (application debug, mass erase command, factory reset command, and TI failure analysis) may be individually enabled, disabled, or (in some cases) enabled through password authentication, providing considerable flexibility to tailor the device behavior to specific use-cases.

When to Use This State

Level 1 is well suited for restricted prototyping/development scenarios and for mass production scenarios where the desire is to retain certain SWD functions (such as factory reset and TI failure analysis) while disabling other functions (such as application debug). Common examples of Level 1 customized configurations are given in

Table 1-6. Examples of Level 1 Configurations

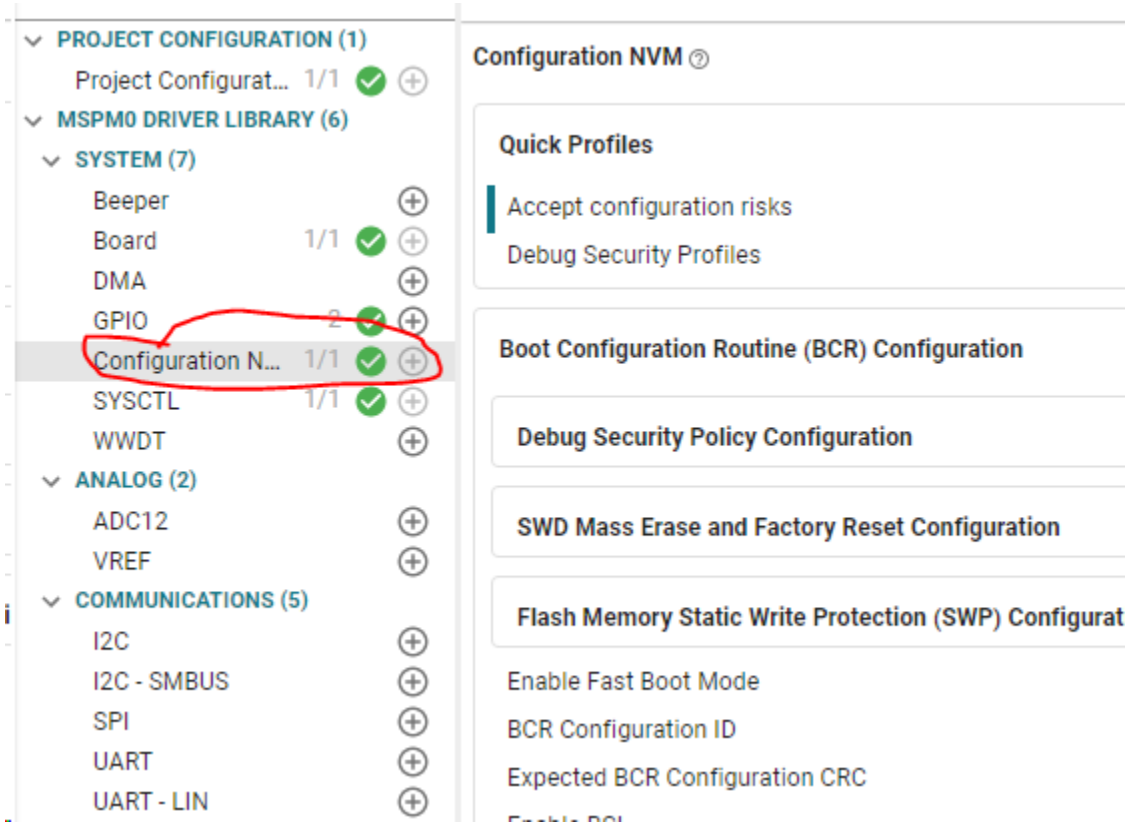
Level 1 Scenario	Configuration			
	App Debug	Mass Erase	Factory Reset	TI FA
This scenario restricts debug access with a user-specified password, but it leaves the factory reset and TI failure analysis available. This configuration allows field debug (with password), and it also allows the device to be brought back to the default "Level 0" state through factory reset.	EN with PW	DIS	EN	EN
This scenario does not allow debug. It does allow factory reset, but only with a user-specified password. This provides a way to open up a device in the field by clearing the MAIN memory contents and bringing the device back to a "Level 0" state if the password is known. Importantly, even if the factory reset password were compromised, it would not be possible for an attacker to read proprietary information in the MAIN flash memory.	DIS	DIS	EN with PW	EN
This scenario does not allow debug and it does not allow TI failure analysis. This prevents TI from performing a factory reset and further FA activities on the device, unless the user executes a factory reset with their user-specified password before returning the devices to TI for FA.	DIS	DIS	EN with PW	DIS

Note

Level 1 is the recommended configuration for most standard production use-cases. For applications which do not require secure boot, TI recommends using Level 1 in production with factory reset left enabled (with password) and TI failure analysis left enabled. In such a configuration, the device may be recovered to a less restrictive state after provisioning either by the user (with password) or by TI (through the failure analysis return flow). In use-cases requiring maximum secure boot assurance, a more restrictive Level 1 or Level 2 may be used for production, with the trade-off that devices may not be recoverable to a less restrictive state once provisioned.

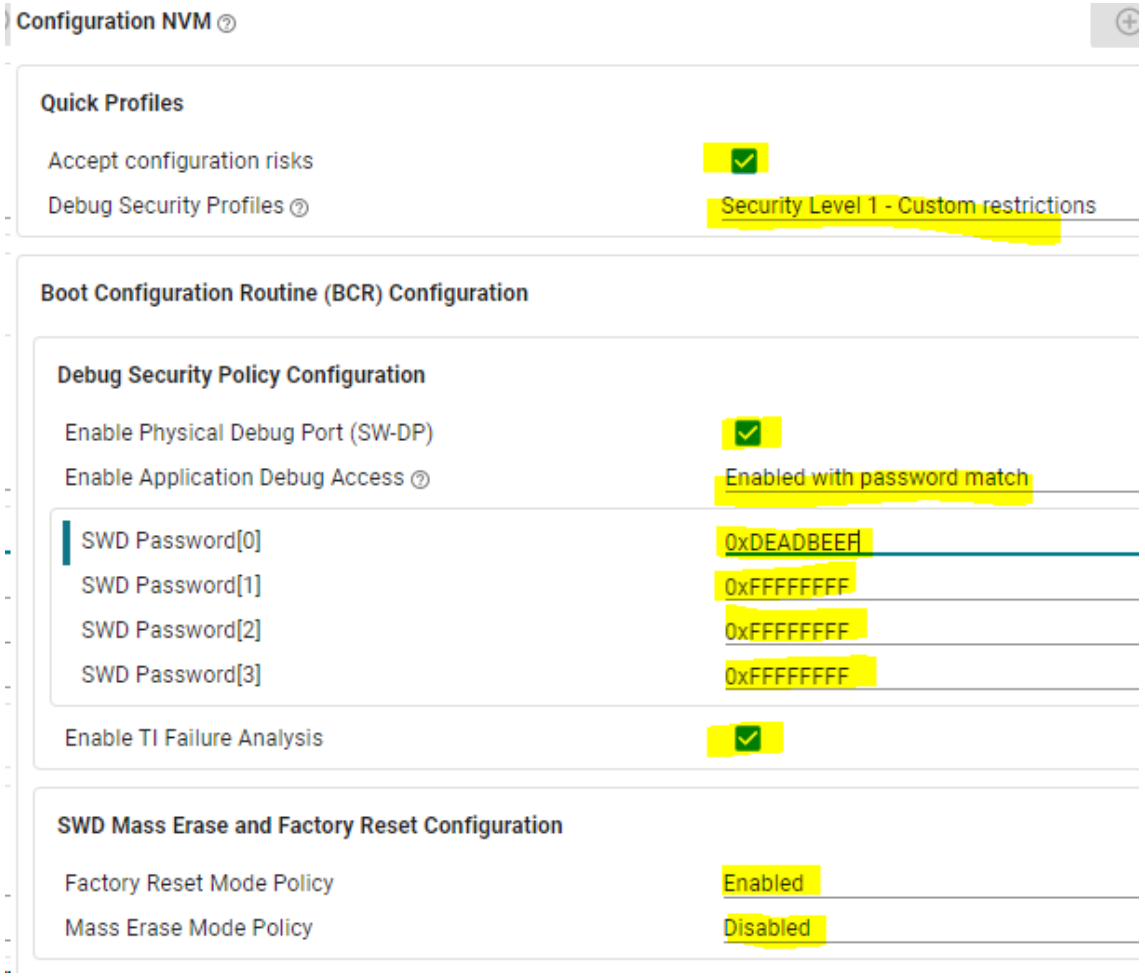
Sysconfig – Add NON-MAIN Configuration

- Sysconfig selection
  - Note: First time you will be asked to check “Accept Configuration risks”



Sysconfig – Select Level 1 Custom Features

- Required feature selections
  - Debug Secure Policy = level 1
  - Enable Physical Debug Port
  - Enable Application Debug Access with password match
  - Create 128bit PW
  - Enable TI Failure Analysis
  - Enable Factory Reset Mode Policy
  - Disable Mass Erase Mode Policy

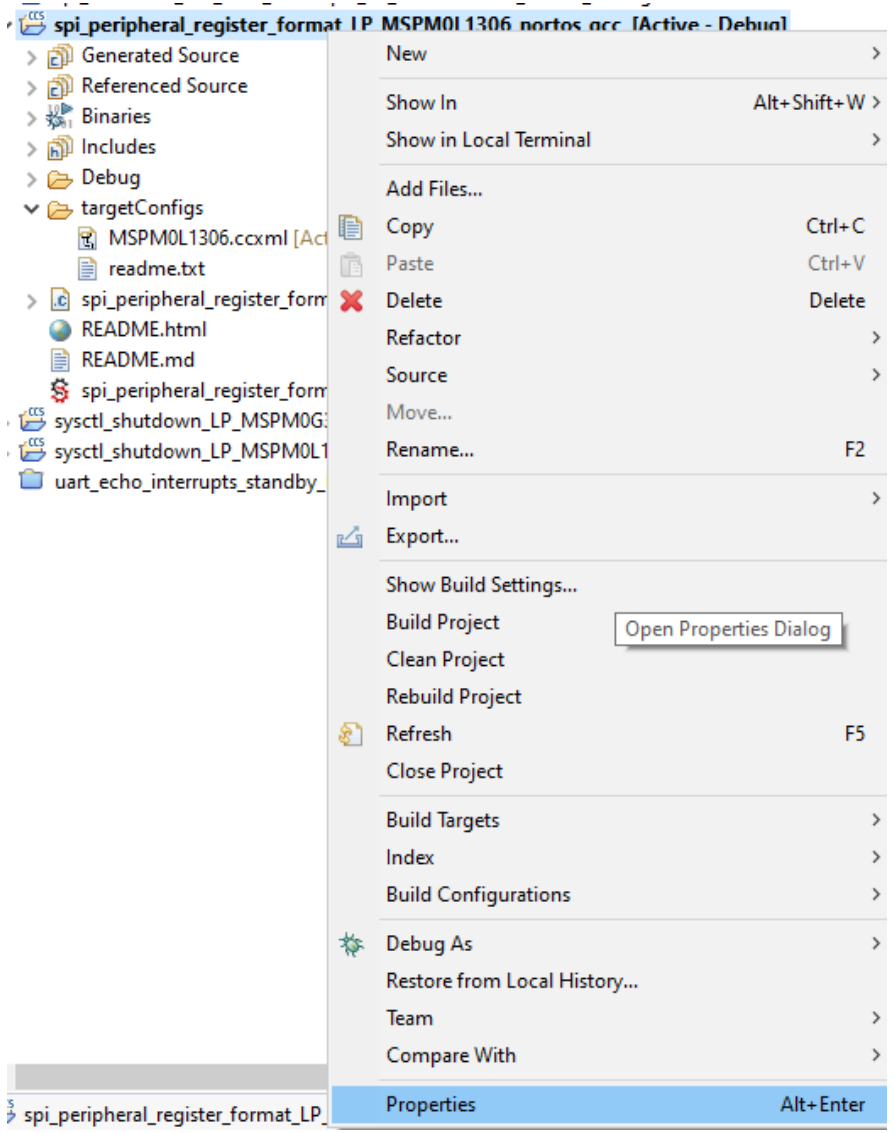


Sysconfig – Enable NON-MAIN Erase

- By default, target configuration (debugger/programmer tool settings) allows only erase of MAIN memory.
  - This protects any customization you may have set in NON-MAIN from being erased
- In order to write your custom Level 1 NON-MAIN configuration you need to allow your debugger/programmer access.
- See next slide

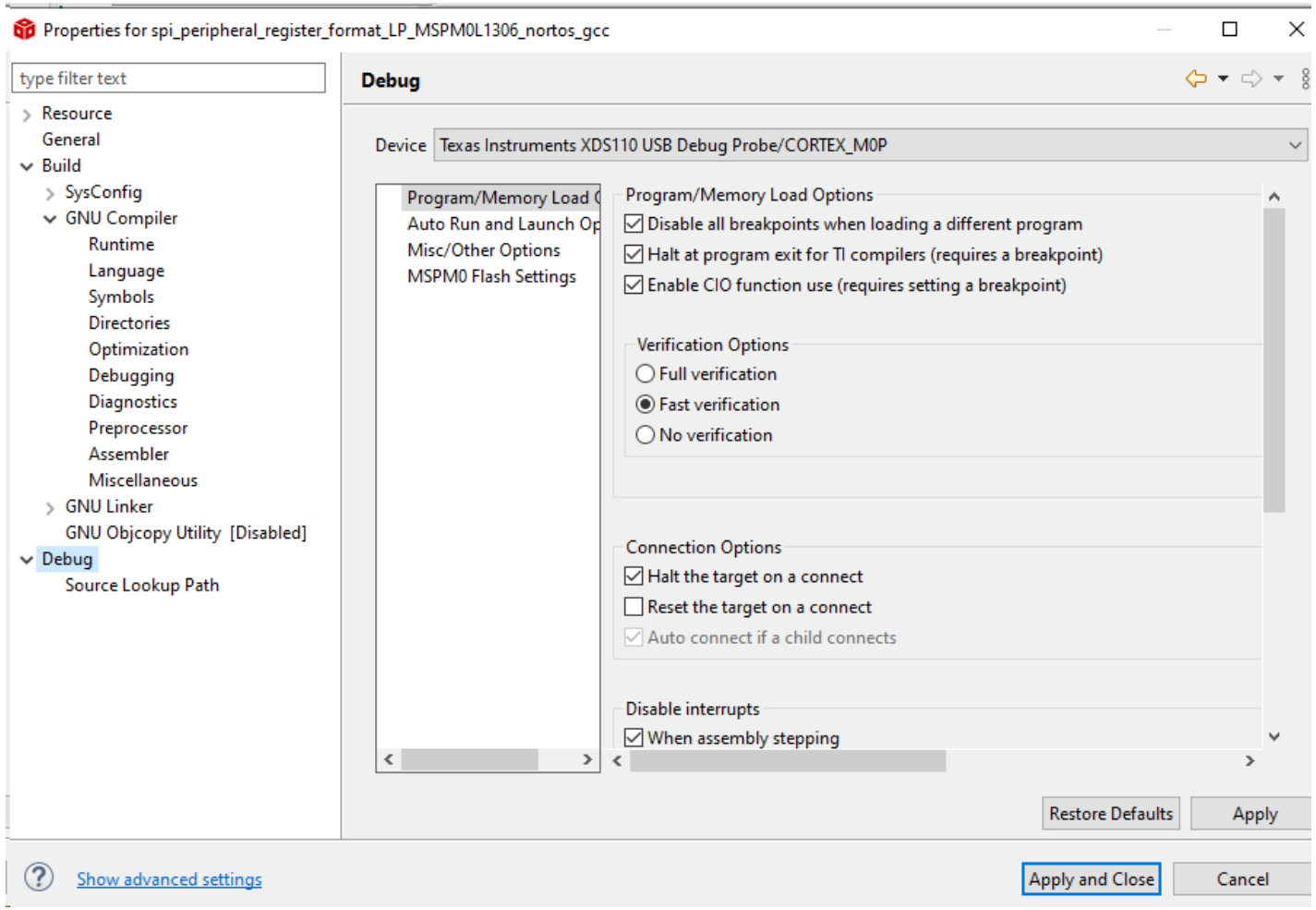
Sysconfig – Enable NON-MAIN Erase

- Right-click on your project name
- Select Properties from the drop-down



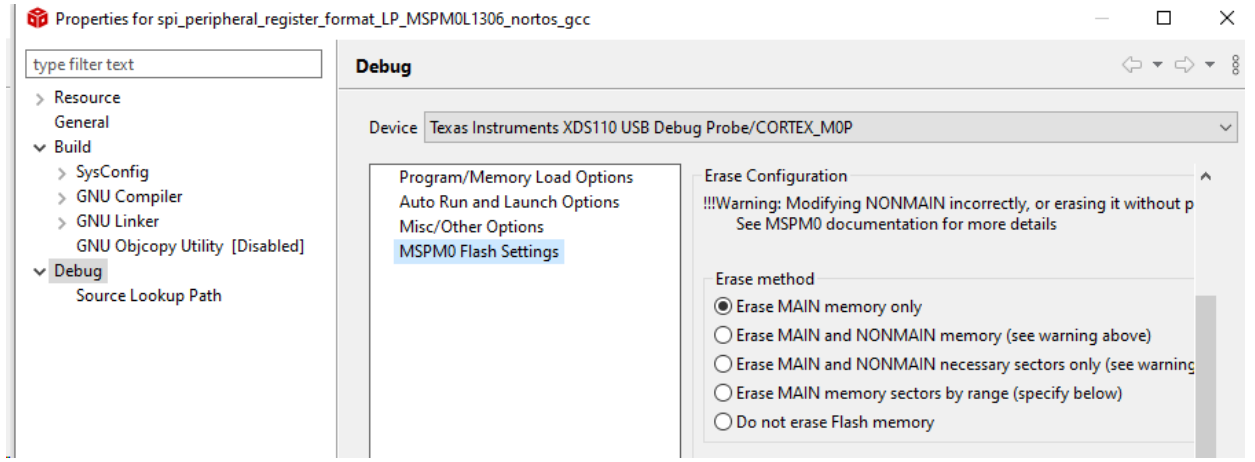
Sysconfig – Enable NON-MAIN Erase

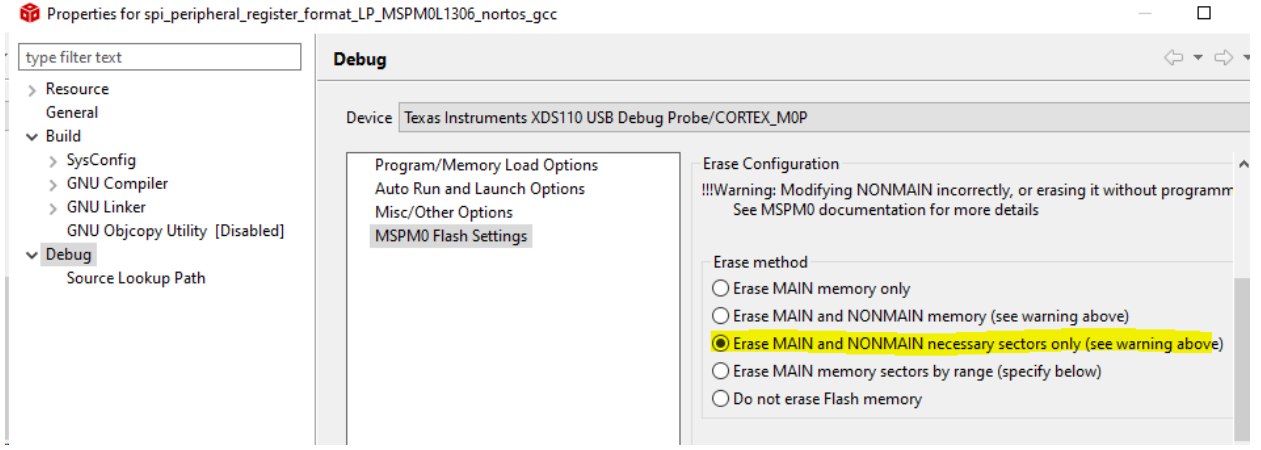
- Select Debug



Sysconfig – Enable NON-MAIN Erase

- Select MSPM0 Flash Settings
- Click Erase MAIN and NON-MAIN necessary sectors only





Sysconfig – Verify SWD Access is protected

- Power cycle the MSPM0
- Attempt to re-program with a different project (one without a PW)
- You should see a target connection error