Registers	Description
UICR.APPROTECT UICR.SECUREAPPROTECT	Hardware control of RRAMC ERASEALL protection in addition to access ports. A device reset is required for this configuration to take effect. Any value other than `Unprotected` disables RRAMC ERASEALL.
UICR.ERASEPROTECT	Hardware control of RRAMC ERASEALL and CTRL-AP ERASEALL protection. A device reset is required for this configuration to take effect. Any value other than `Unprotected` disables the erase all operations.
TAMPC.PROTECT.ERASEPROTECT	Software control of RRAMC ERASEALL and CTRL-AP ERASEALL protection. The register can be locked.

Table 74: Erase protection

The ERASEALL protection is illustrated in the following figure:

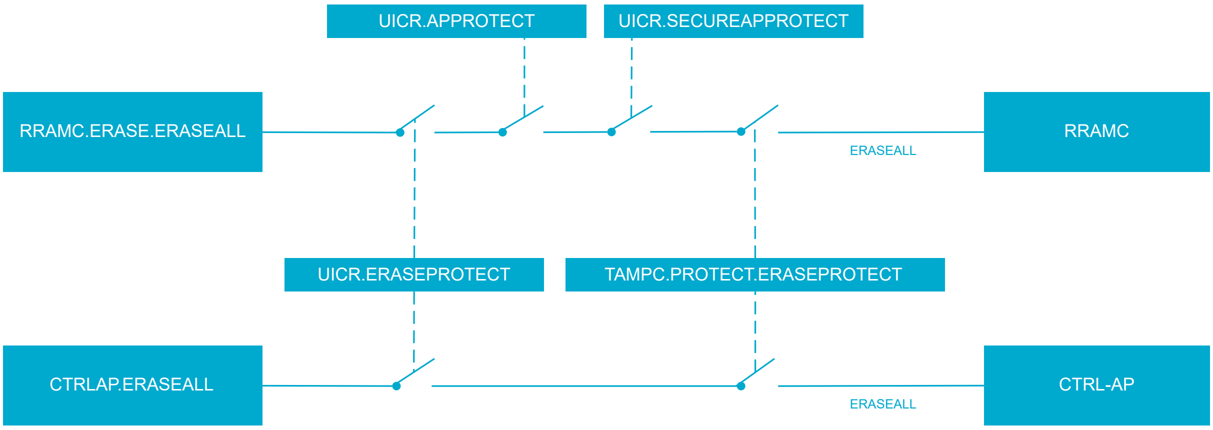

Figure 167: ERASEALL protection overview

The reset behavior of the TAMPC access port and ERASEALL protection is defined in Signal protector on page 194. On-chip software must write to the TAMPC registers before a debug access port is opened.

The access port remains open after the completion of the CTRL-AP.ERASEALL operation. CTRL-AP temporarily removes the access port protection until certain conditions are met, after which the protection will be reinstated. The AHB-AP will be protected when one of the following conditions are met:

- Power-on reset
- Brownout reset
- Watchdog timer reset
- Pin reset

The following figure shows how a device with access port protection enabled can be erased, programmed, and configured to allow debugging. The access port state is determined by operations sent from the debugger and registers written by firmware. Reset in the following figure refers to any of the conditions previously listed for AHB-AP protection. When writing to the TAMPC, the software must first disable write protection, then write the new values. For more details, see TAMPC — Tamper controller on page 192.