When an internal tamper event is detected, one of the following will occur:

- A TAMPC EVENT is generated.
- A chip reset is triggered and the SECTAMPER value in the reset reason register indicates what happened, depending on the status of the register PROTECT.INTRESETEN.CTRL on page 210.

The internal tamper reset enable signal INTRESETEN is enabled from reset.

7.8.6.4 Signal protector

The device implements detectors to protect selected signals that control critical device features.

The signal protector implements one detector per protected signal to detect unintentional value changes in that signal. The detector notifies TAMPC if a protected signal changes value caused by tampering. The detectors are enabled from reset and can be disabled using the register , which is for debugging purposes only. A detected unintentional value change in any of the protected signals leads to an internal tamper event where one of the following occur:

- A TAMPC event is generated.
- A chip reset is triggered and the SECTAMPER value in the reset reason register indicates what happened, depending on the status of the register PROTECT.INTRESETEN.CTRL on page 210.

The INTRESETEN register is enabled from reset. The PROTECT.<component>.STATUS registers indicate which protected signal had an unintentional value change when the register INTENRESETEN is disabled.

The signal protector implements a two stage write cycle to change the value of a protected signal, in addition to a required write key which must be included for all register writes. The two stages are the following:

1. Initial register write to clear the write protection.
2. Register write to change the signal's value.

Write Clear to the WRITEPROTECTION field in the PROTECT.<component>.CTRL register to clear the write protection in the first register write. Then write to the VALUE and LOCK fields in the next register write operation.

> **Note:** It is required to clear the WRITEPROTECTION field before any updates to the VALUE and LOCK fields are accepted by the register.

The write protection is automatically re-enabled after the subsequent write to change the VALUE field when the register write does not include the Clear value in the WRITEPROTECTION field.

The LOCK field controls a lock feature which prevents further updates to the VALUE and LOCK fields until a reset with the required reset source for the specific signal is issued.

A WRITEERROR event is generated for any of the following conditions:

- Register write does not have the correct write key
- Write protection is active and the write operation does not contain the value to clear the write protection
- The lock is enabled

The sequence to change the VALUE or LOCK fields in the PROTECT.<component>.CTRL registers is as follows:

1. Write Clear to the WRITEPROTECTION field and KEY to the KEY field.
2. Write Disabled to the WRITEPROTECTION field, KEY to the KEY field, and KEY to the desired LOCK and VALUE fields.

7.8.6.4.1 Debugger signals

TAMPC provides protection for the following Arm CoreSight™ debugger signals.