Bit number				31	30	29	28	27	26	25	24	23	22	21	20	19	18	17	16	15	14	13	12	11	10	9	8	7	6	5	4	3	2	1	0
ID				B	B	B	B																									A	A	A	A
Reset 0x00000001				**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**0**	**1**
ID	R/W	Field	Value ID	Value																															
A	R	PROTVSN																																	
			SWDPv2	1																															
B	R	TINSTANCE																																	
				Target instance.																															

9.2 Access port protection

The access ports can be protected to secure the internal assets and resources of the device. While the control access port (CTRL-AP) is always accessible from an external debugger, the system applies various protection mechanisms to control and restrict access to the individual AHB access ports. These mechanisms ensure both secure and non-secure access can be selectively managed and protected.

Protection is controlled by specific registers, which enable or disable debug access at different levels. These registers are part of UICR and TAMPC. The access port is normally protected. The hardware and software configurations of these registers control the access protection policies as shown in the following table.

Registers	Description
UICR.APPROTECT	Hardware control of non-secure debug access. A device reset is required for this configuration to take effect. `Unprotected` – CPU controls DBGEN/NIDEN, locks disabled. Other values – DBGEN/NIDEN disabled and locked.
TAMPC.PROTECT.DOMAIN[0].DBGEN TAMPC.PROTECT.DOMAIN[0].NIDEN	CPU control of non-secure debug access. The registers can be locked.

Table 71: Non-secure Arm Cortex-M33 AHB-AP debug access

Registers	Description
UICR.SECUREAPPROTECT	Hardware control of secure debug access. A device reset is required for this configuration to take effect. `Unprotected` – CPU controls SPIDEN/SPNIDEN, locks disabled. Other values – SPIDEN/SPNIDEN disabled and locked.
TAMPC.PROTECT.DOMAIN[0].SPIDEN TAMPC.PROTECT.DOMAIN[0].SPNIDEN	CPU control of secure debug access. The registers can be locked. Non-secure invasive debug access must be enabled for secure debug access to be enabled.

Table 72: Secure Arm Cortex-M33 AHB-AP debug access