[Linux] On-chip breakpoints do not stop the program execution during kernel boot

2022-01-12 - Comments (0) - OS-aware debugging

On-chip breakpoints can be removed by the kernel during boot:

- The Linux kernel resets on **Arm** the breakpoints as well as the **Vector Catch Register (VCR)** when booting if **CONFIG_HAVE_HW_BREAKPOINT** is enabled in the kernel configuration. See arch//kernel/hw_breakpoint.c. This can be detected on Armv8 by enabling the option **TrOnchip.Set TDA ON**.
- A similar problem can also be seen on **Intel x86** when the debug registers are cleared during boot. Please refer to arch/x86/include/asm/debugreg.h. This can be detected by enabling the option **TrOnchip.Set GeneralDetect ON**.