

RS232-T300

🔑 Trojan Description

- 🔑 Trojan trigger is a 32-bit counter inserted in the transmitter part of micro-UART core. The counter is increased by 1 after each transmission and the Trojan becomes activated when the counter reaches 32'hFFFFFFF. After Trojan activation, Trojan payload replaces the 7th bit of all data being transmitted afterward.

🔑 Trojan Taxonomy

- 🔑 Insertion phase: Design
- 🔑 Abstraction level: Register-transfer level (RTL)
- 🔑 Activation mechanism: Internally time-based triggered
- 🔑 Effect: Information leakage
- 🔑 Physical characteristic: Functional

Functional

The number of Transmitted	Trojan activation	Payload Change	Simulation Length (No. Clock)	Length of each Transmission
954 545	0	0	168 000 000	176