

Ukryte funkcjonalności w układach scalonych

mgr inż. Tadeusz Andrzejewski

Dane potrzebne do odtworzenia schematu elektrycznego urządzenia to informacje zdobyte na podstawie zewnętrznej obserwacji:

- typów zastosowanych układów,
- ilości układów,
- ilości wyprodukowanych urządzeń,
- not aplikacyjnych dostarczanych przez producentów układów.

Miejsca, w których mogą być umieszczane aplikacje:

- procesory,
- kontrolery transmisyjne,
- interfejsy do pamięci.

Aplikacje mogą być uruchamiane ustalonymi sekwencjami kluczowymi znajdującymi się wśród transmitowanych danych.

Sekwencje kluczowe mogą mieć duże długości - praktycznie niemożliwe jest wykrycie istnienia takiej aplikacji metodą podawania różnych sekwencji.

Funkcjonalności ukrytych aplikacji:

- podglądanie transmitowanych danych,
- obserwowanie pinów - dostarczanie dodatkowych danych umożliwiających określenie wcześniej nieznanych szczegółów dotyczących schematu elektrycznego urządzenia,
- reakcja na umówioną sekwencję kluczową – zmiana podstawowych funkcjonalności układu.

Przeciwdziałanie:

- ukryte funkcjonalności są trudne do wykrycia,
- stosowanie na wejściach nietypowych połączeń,
- ciągła obserwacja zdarzeń w czasie eksploatacji urządzenia – badanie nietypowych zdarzeń.