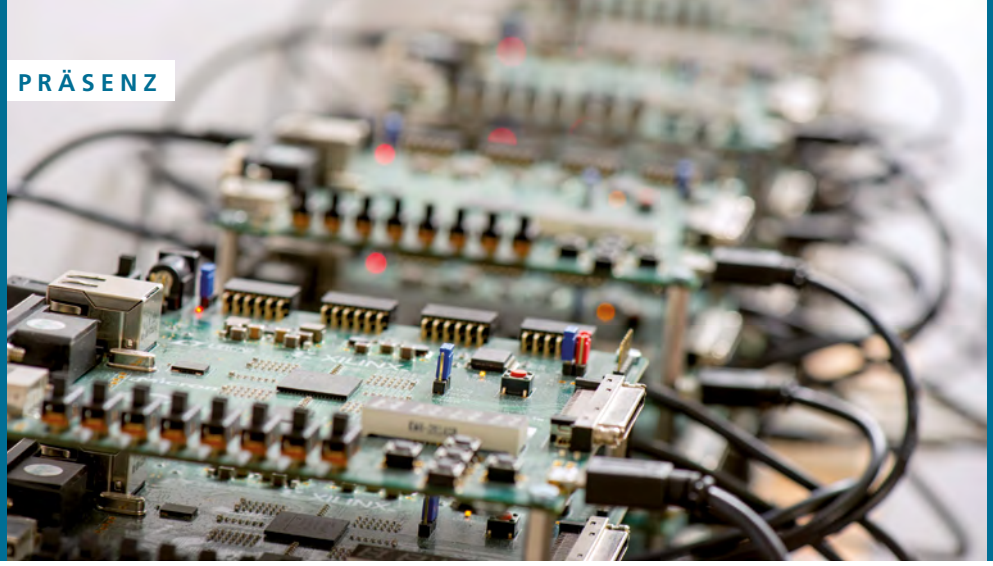
PRÄSENZ



IT-SICHERHEIT IN KOMPLEXER UMGEBUNG

ABSICHERUNG FPGA-BASIERTER SYSTEME

Die Herausforderung: Flexible und sichere FPGA-Systeme (Field Programmable Gate Array) bauen. Rekonfigurierbare Hardware-Bausteine, sogenannte FPGAs, ermöglichen die Beschleunigung von Netzwerkfunktionen. Ihre Programmierbarkeit erlaubt neue Flexibilität. Ein Vorteil, der auch Angriffsmöglichkeiten bietet. Für die IT-Sicherheit zeigt das: Es braucht ein hohes Maß an Erfahrungswissen. Dieses Seminar stattet Sie damit aus. In einem Vorgespräch lassen sich die Inhalte des Seminars deshalb unternehmensspezifisch anpassen.

Inhalte des Seminars

Einführung in die Marktanalyse FPGA

- Einordnung mit einem unabhängigen Marktüberblick FPGA

Angriffe auf FPGA

- Reverse Engineering
- Seitenkanalangriffe
- Fehlerangriffe

Sicherheitskonzepte für FPGAs in Embedded Systems

- Secure HDL Coding Style
- Systematische Prüfung der Sicherheit des Gesamtsystems

FPGA Auswahlkriterien

- Sicherheitsfunktionen kommerziell verfügbarer FPGAs

Ihr Nutzen

» Nach dem Seminar haben Sie einen Überblick über aktuelle Angriffe auf FPGAs und können diese verstehen.
» Sie wissen, welche Gegenmaßnahmen mit aktuellen Chips implementiert werden können.
» Sie wissen, wie Sie ein sicheres FPGA-basiertes System designen können.
» Sie sind in der Lage, anhand von relevanten Kriterien den geeigneten FPGA für die Absicherung Ihres Systems auszuwählen.

INFORMATIONEN IM ÜBERBLICK

Idealerweise Grundlagen IT-Security und FPGA Design (wird optional vermittelt)

Embedded Systems & Hardware Architekten* innen und Entwickler* innen, Technische Leitung, Fachexperten/innen

1–2 Tage Präsenz

600,– bzw. 1200,–

Garching bei München, inhouse

Veranstaltet durch

Fraunhofer AISEC

Referenten:

Nisha Jacob Kabakci,
wiss. Mitarbeiterin
Fraunhofer AISEC

Robert Hesselbarth,
wiss. Mitarbeiter
Fraunhofer AISEC

Weitere Infos und aktuelle Termine buchen unter:

www.cybersicherheit.fraunhofer.de/eingebettete-systeme-fpgas