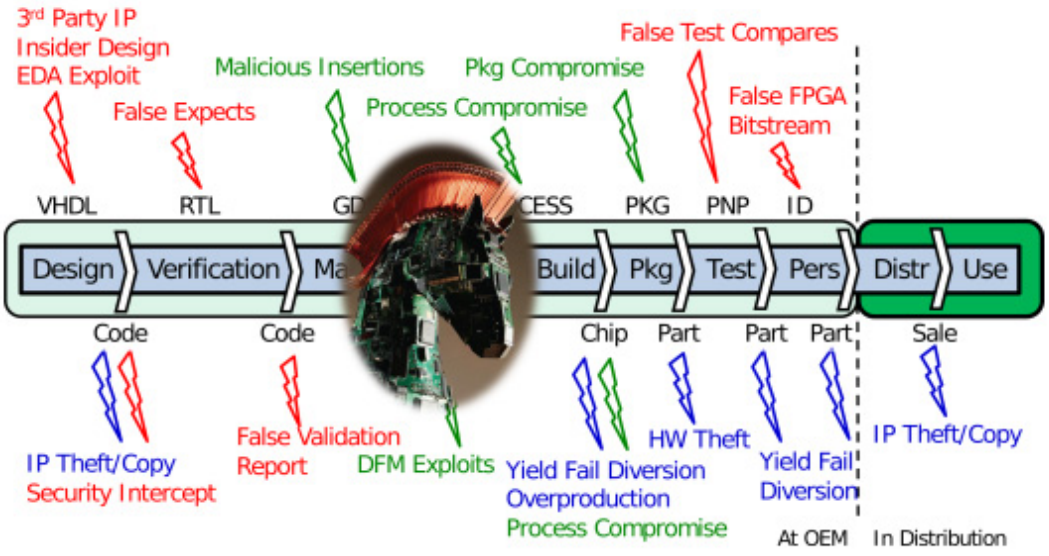
Fakultät Elektrotechnik und Informationstechnik
Institut für Feinwerktechnik und Elektronik-Design

TECHNISCHE UNIVERSITÄT DRESDEN

Einladung zum 207. Institutskolloquium

Thema:	**Hardware Security: Eine Einführung zu Sicherheit und Schutz von elektronischen Schaltkreisen**
Vortragender:	**Dr.-Ing. Johann Knechtel, New York University Abu Dhabi**
Leitung:	**Prof. Dr.-Ing. habil. Jens Lienig**
Zeit / Ort:	**16. März 2018, 14 Uhr im Barkhausenbau II/26**

Integrierte elektronische Schaltkreise (ICs) dominieren den heutigen Alltag – ohne sie wäre der allgegenwärtige und rasante technische Fortschritt nicht denkbar. Damit werden ICs jedoch auch zu kritischen und wertvollen Komponenten jeglicher Informationsverarbeitung, deren gewünschte Funktionsweise sowie deren geistiges Eigentum es zu bewahren gilt. Konkrete Risiken ergeben sich zum Beispiel durch böswillige Modifizierungen von ICs während des Entwurfs oder der Herstellung, der unlizenzierten Überproduktion von Schaltkreisen, dem Diebstahl des geistigen Eigentums, oder aber auch dem Abgreifen von sensiblen Daten zur Laufzeit.



Der etwa 40-minütige Vortrag gibt eine Einführung zum Thema „Hardware Security“, wobei anfänglich die Grundprinzipien von Sicherheit, Vertrauenswürdigkeit und Schutz im Kontext von integrierten Schaltkreisen aufgedeckt werden. Diese Prinzipien sind vor allem durch die der Herstellung zugrundeliegenden Prozesskette bedroht. Der Vortrag umfasst motivierende Fallbeispiele als auch neuartige Forschungsansätze bezüglich Hardware Security. Ein Ausblick auf zukünftige Entwicklungen rundet den Vortrag ab.