"Ich bin sicher“ - Selbstverifiziernde Cyber-Physiche Systeme

Die Sicherheit von Cyber-Physischen Systemen kann duch formale Verifikation wesentlich erhöht werden. Um der hierbei auftretenden Zustandsexplosion entgegenzuwirken haben wir in den letzten Jahren Techniken der Selbstverifikation entwickelt, in denen das System sich zur Laufzeit selbst verifiziert. Durch die Instantiierung von Variablen zur Laufzeit wird der Zustandsraum drastisch verkleinert, und damit formale Verifikation wieder möglich. Hierbei können entweder Variablen instantiiert werden, derenWerte über längere Zeit konstant bleiben, oder deren Instantiierung den Zustandsraum besonders drastisch verkleinert. Eine Verfeinerung dieser Technik berücksichtigt die zeitliche Dimension: wir verifizieren das Systemverhalten für genau die Zustände, die innerhalb eines gegeben Zeitraums erreicht werden können. Diese Techniken erlauben es auch insbesondere, Systeme zu verifizieren, über deren Struktur wenig bekannt ist, insbesondere solche, deren Kontrollalgorithmus KI-basierten Verfahren nutzt. Der Vortrag stellt die grundlegenden Techniken der Selbstverifikation vor und illustriert die Herangehensweise an Fallstudien.