Penetration Test-Driven Safety and Security System Improvements for Cyber-Critical Systems (Pets3)

PetS3 - „Penetration Test Driven Safety and Security System Improvements for Cyber-Critical Systems“ ist das mittelstandsorientierte Forschungsvorhaben mit Multiplikator-Wirkung zu den Hersteller- und Betreiberkonzernen cyber-kritischer Systeme in Bayern:

Aufgrund der fortschreitenden Vernetzung sind Cyber-Attacken eine wachsende Bedrohung einer Vielzahl von Anwendungsgebieten wie z.B. Vernetztes Fahrzeug oder Smart Metering. Gemeinsame Konzepte der funktionalen Sicherheit (Safety) und der IT-Sicherheit (Security) sind für diese Gateway-basierten Systeme erforderlich. Ziel des Forschungsvorhabens ist es, Angriffe auf die IT-Sicherheit von Systemarchitekturen vernetzter cyberkritischer Systeme zu erforschen, da die Wechselwirkung zwischen funktionaler Sicherheit und IT-Sicherheit in diesem Kontext weitestgehend unbekannt ist.

Zentraler Forschungsgegenstand ist die ganzheitliche Analyse der Sicherheits-technologien, der Gateway- Strukturen und der korrespondierenden System-entwicklungsprozesse. Ausgehend von Schwachstellen und Bedrohungsanalysen, sowie Penetrationstests und Architekturanalysen werden Anforderungen für System-architekturen, Sicherheitstechnologien und Prüfverfahren, sowie für ein Reifegradmodell abgeleitet. Es wird ein Schwachstellen- und Bedrohungskatalog entwickelt, der die Grundlage für eine automatisierte Analyse der funktionalen Sicherheit sowie der IT-Sicherheit bildet und damit einen zentralen Beitrag zur Risikobewertung von cyber-kritischen Systemen darstellt.

Durch die Architektur- und Bedrohungsanalyse funktional sicherer Systeme werden die Möglichkeiten und Grenzen der Absicherung durch Lösungskonzepte erforscht. Die Erkenntnisse aus Schwachstellen- und Bedrohungsanalysen werden kontinuierlich in ein Reifegradmodell hinsichtlich der funktionalen Sicherheit und der IT-Sicherheit („safe and secure“) integriert und um aktuelle Erkenntnisse aus der IT Sicherheitsforschung z.B. „Security by Design“ angereichert. Damit gelingt die beurteilende Vermessung des Reifegrads von Entwicklungsprozessen und Produkten für cyber-kritische Systeme.

Die Ergebnisse des PetS3 Forschungsvorhabens sind:

1. Penetrationswerkeuge, welche die Möglichkeit bieten automatisierte IT-Sicherheitstests mit Beurteilung der funktionalen Sicherheit von vernetzten cyber-kritischen Systemen durchzuführen.
2. Ein Geschäftsmodell zur gemeinsamen Zertifizierung der IT-Sicherheit und funktionalen Sicherheit für Audits und Assessments durch mittelständische Unternehmen entwerfen.
3. Ein Reifegradmodell zur Vermessung von Prozessen und Verfahren der Entwicklung neuer cyber-kritische System-Produkte.