# Decentralized Anomaly Detection

**Motivation:** In heutigen IT-Systemen kommt eine ständig wachsende Anzahl Rechner zum Einsatz. Zudem nehmen der Grad an Vernetzung und die Zahl von Abhängigkeiten zwischen Rechnern zu. Beides erschwert die Aufgabe, derart komplexe IT-Systeme zu schützen. Hinzu kommt, dass IT-Systeme heute kaum mehr von in der Außenwelt existierenden Gefahren abschottbar sind. Gründe sind die räumliche Ausdehnung der Netze und deren Interaktion mit ihrer Umwelt. Zur Kostenersparnis werden zudem ehemals physikalisch getrennte Rechner und Netzwerke konsolidiert, was zu einer Aufweichung der Sicherheit führen kann. Auch die im Projekt betrachteten IT-Systeme von Flugzeugen und Automobilen sind derartigen Veränderungen unterworfen.

Diese Entwicklungen schaffen neue Gefahrenpotenziale und Risiken in Bezug auf die Informations- und Betriebssicherheit der IT-Systeme. Für Angreifer entstehen neue Angriffsmöglichkeiten, gegen die bisher nur unzureichend geschützt werden kann. Stetiges Überwachen von Komponenten, frühzeitiges Erkennen von Angriffen und umfassende Bewertung des Sicherheitsniveaus des Gesamtsystems sind daher unumgänglich.

**Ziele:** Die zunehmende Vernetzung von Komponenten bietet aber auch Chancen für neuartige und umfassende Ansätze der Anomalieerkennung. Viele eingesetzte Komponenten verfügen über ungenutzte Rechenkapazitäten. Die Kernidee des Projekts DecADe ist, diese ungenutzten Kapazitäten zur dezentralen und autonomen Überwachung des Gesamtsystems zu nutzen.

Im Projekt DecADe werden vorrangig zwei unterschiedliche Anwendungsfälle untersucht: vernetzte IT-Systeme in Flugzeugen und in Automobilen. In den beiden Anwendungsfällen werden verteilte Controller verwendet, die eine große Menge unterschiedlicher Daten erfassen und eine Vielzahl an Funktionen bereitstellen. Trotz begrenzter Ressourcen sind die Controller nicht immer ausgelastet. So kann ungenutzte Rechenkapazität anderweitig eingesetzt werden, beispielsweise um zusätzliche Monitoring-Daten zu erheben und diese auf Anomalien hin zu untersuchen.

## Eckdaten

**Kurztitel**

DecADe

**Forschungsschwerpunkt**

Digital Technologies

**Laufzeit**

01.06.2016 - 31.05.2019

**Fördergeber**

Bundesministerium für Bildung und Forschung

**Projektträger**

VDI/VDE Innovation + Technik GmbH

**Projektleitung**

Prof. Dr. Martin Schramm

## Ziele

- Amplifizierung der Anomalieerkennung
- Anderweitige Nutzung von nicht gebrauchter Rechenkapazität
- Die Dezentrale und autonome Überwachung des Gesamtsystems zur Vollendung dieses Glanzstückes