

Automotive MILS

Jean-Pierre Seifert¹ Michael Peter²

Abstract: Ohne Elektronik, die im Laufe der letzten 30 Jahre ein unverzichtbarer Bestandteil im Automobilbau geworden ist, wäre eine Vielzahl von Innovationen wie ABS, EPS etc. undenkbar gewesen. Dieser Trend wird sich aller Wahrscheinlichkeit nach auf absehbare Zeit mit Fahrerassistenz- und Infotainmentsystemen fortsetzen, wenn nicht sogar verstärken. Vor dem Hintergrund der stark wachsenden Systemkomplexität ist die bisherige Annahme, dass alle Komponenten als vertrauenswürdig betrachtet werden können, fragwürdig. Die daraus resultierenden Fragen nach der Systemsicherheit und -verlässlichkeit können ohne geeignete Gegenmaßnahmen zu einer erheblichen Innovationsverlangsamung führen.

Angesichts der sich abzeichnenden Anforderungen, mehr Funktionen auf einer Plattform zu integrieren, schlagen wir den Einsatz von MILS (multiple independent levels of security), einer bewährten Sicherheitssystemarchitektur, im automobilen Umfeld vor. Wir skizzieren anhand von drei Beispielen wie mit Hilfe von MILS Sicherheits- und Verlässlichkeitsrisiken begegnet werden kann: Absicherung von Kommunikation in offenen Netzen, Einsatz von Standardbetriebssystemen (Linux) und Softwareaktualisierung (FOTA).

¹ Technische Universität Berlin, jpseifert@sec.t-labs.tu-berlin.de

² Technische Universität Berlin, peter@sec.t-labs.tu-berlin.de