

ZeMoSS-Workshop: Zertifizierung und modellgetriebene Entwicklung sicherer Software

Michaela Huhn¹

Stefan Gerken²

Carsten Rudolph³

¹ Institut für Informatik, Technische Universität Clausthal

² IC MOL RA R&D, Siemens AG, Braunschweig

³ Fraunhofer Institut für Sichere Informationstechnologie (SIT), Darmstadt

Software ist ein wesentlicher Innovationsfaktor bei vielen technischen Produkten und Infrastrukturen.

Mit dem vielfältigen Einsatz softwaregesteuerter Systeme wachsen die Qualitätsanforderungen, insbesondere in den Bereichen funktionale Sicherheit und Informationssicherheit. In der Luft- und Raumfahrt, der Energieerzeugung und im Schienenverkehr, aber auch in der Medizintechnik wie auch in den Bereichen Automobiltechnik und mobile Systeme sind die Zertifizierung und der Nachweis der Sicherheit kritischer Systeme und softwarespezifische Sicherheitsnormen international etabliert und bindend. Mehrere domänenübergreifende Herausforderungen bei der Entwicklung sicherer Software werden im Workshop adressiert:

- Modellgetriebene Software-Entwicklung wird in der Industrie immer wichtiger und für höhere Sicherheitsanforderungsstufen seit langem in Sicherheitsnormen als dringend empfohlen klassifiziert. Normen können aber nur unzureichend auf den Stand von Wissenschaft und Technik eingehen. Neue Methoden und Werkzeuge müssen im Zertifizierungsprozess akzeptiert werden, auch wenn zu ihnen keine normativen Aussagen vorliegen. Somit steht einer Qualitätserhöhung von Software in sicherheitsrelevanten Anwendungen durch neue Methoden immer die fehlende normative Erwähnung dieser Methode gegenüber.
- Durch die zunehmende Vernetzung innerhalb kritischer Infrastrukturen und die Anbindung mobiler Endgeräte werden viele Anwendungen erst ermöglicht, aber es entstehen auch neue Risiken aus der wechselseitigen Abhängigkeit von Informationssicherheit und funktionaler Sicherheit. Hier sind neue Methoden gefragt, die eine integrierte Modellierung von Safety und Security in der Risikoanalyse, der Entwicklung und dem Nachweis unterstützen.

Der ZeMoSS-Workshop soll den Austausch über offene Punkte und Lösungsansätze zu zentralen Herausforderungen in der Software-Entwicklung für sicherheitskritische Systeme und Infrastrukturen domänenübergreifend zwischen Teilnehmern aus Industrie und Forschung fördern.

