Name
Dirk Kuschnerus

Titel der eingereichten Dissertation
Modellierung und Verifikation sicherheitskritischer konfigurierbarer Systeme in der Prozessmesstechnik

Kurzfassung
Diese Arbeit führt eine Methode zur modellgetriebenen Entwicklung und Verifikation von Systemen der Prozessautomatisierung ein. Die Prozessautomatisierung unterscheidet sich von anderen Domänen durch eine Kombination spezieller Eigenschaften. Die inhärente Integration von physikalischen Prozessen mit softwaregestützten Regelungen kennzeichnet Systeme der Prozessautomatisierung als cyber-physische Systeme, deren Entwicklung und Verifikation die Einbeziehung kontinuierlicher und diskreter Dynamik erfordert. Aufgrund der potentiellen Gefährdung von Menschen und Umwelt durch die in den Prozessen verwendeten Stoffe unterliegen Systeme der Prozessautomatisierung meist Standards zur funktionalen Sicherheit wie DIN EN 61508 und DIN EN 61511. Die zur Regelung der Prozesse verwendeten CPS müssen daher hinsichtlich ihrer Fähigkeit verifiziert werden, die Systeme bei Auftreten eines potentiell gefährlichen Ereignisses in einen sicheren Zustand zu überführen. Darüber hinaus bestehen Systeme der Prozessautomatisierung typischerweise aus einer Menge generischer Komponenten, die zur Integration in eine konkrete Applikation konfiguriert werden. Die durch die Vielfalt an Anwendungsfällen und damit verbundenen Anforderungen entstehenden statischen und dynamischen Daten innerhalb der Systemkomponenten erzeugen einen hohen Grad an Variabilität, der bei der Sicherheitsverifizierung berücksichtigt werden muss. Diese wiederum muss, bedingt durch die Einbindung konfigurierbarer Geräte in bestehende Anlagen, eine online durchführbare Sicherheitsverifikation der vorgenommenen Parametrisierung beinhalten.
Zusätzlich zu diesen technischen Herausforderungen weisen Systeme der Prozessautomatisierung typischerweise durch die Aufteilung in Anlagen und dazu gehörigen Verbünden von interagierenden Prozessen eine hohe Komplexität auf, die durch unterschiedliche Verwendung der Entwicklungs- und Laufzeitinformationen durch verschiedene am Prozess beteiligte Rollen verstärkt wird.
Durch die Kombination der inhärenten cyber-physischen Charakteristik, der funktionalen Sicherheit sowie der Konfigurierbarkeit in komplexen, hierarchisch aufgebauten Szenarien stellen Systeme der Prozessautomatisierung hohe Anforderungen an Entwicklungs- und Verifikationsmethoden, die durch vorhandene Ansätze nicht vollständig abgedeckt werden können. Zudem existieren keine Ansätze, die das aus den verschiedenen Rollen und Anlagenelementen ableitbare Domänenwissen bei der Entwicklung und Verifikation verfügbar und im Umkehrschluss die formale Verifikation für Domänenexperten zugänglich machen. Aus dieser Problemstellung heraus leistet diese Arbeit die folgenden Beiträge:

- Erhebung des Stands der Forschung in den Bereichen der aspektorientierten Modellierung von konfigurierbaren, sicherheitskritischen CPS sowie der Sicherheitsverifikation konfigurierbarer CPS anhand einer systematischen Literaturanalyse
- Entwicklung einer domänenspezifischen Modellierungssprache (DSML), die Abstraktionsebenen und Sichten für Systeme der Prozessautomatisierung definiert und das Domänenwissen durch spezielle Modellelemente integriert. Die Integration der Querschnittsfunktionen der funktionalen Sicherheit und Konfigurierbarkeit erfolgt in Form von orthogonalen Aspekten, die eine Trennung von Querschnittsfunktionen und Domänenmodellen und damit eine Reduzierung der Komplexität der Modelle erreicht. Zusätzlich zur Definition der Domänen- und Aspektmodelle erfolgte die Entwicklung eines auf dem Eclipse Modeling Framework basierenden Rahmenwerks zur Spezifikation, Transformation und Verwaltung der in der Arbeit eingeführten Modelle.
- Entwicklung eines Algorithmus zur Konsistenzprüfung, der ausgehend von den Anforderungen der Domäne und den in der DSML spezifizierten Modellen die dynamische Sicherheitskonsistenz der in dieser Arbeit untersuchten Systeme formal nachweist. Dazu untersucht der Algorithmus die Auswirkungen konkreter und symbolischer Konfigurationsdaten auf die Realisierungsmodelle von System- und Sicherheitsfunktionen hinsichtlich einer Veränderung der Ausführungszeit und integriert die gewonnenen Informationen in hybride Automatenmodelle der sicherheitskritischen Regelungsalgorithmen. Basierend auf den Automatenmodellen zeigt der Algorithmus anschließend durch eine Erreichbarkeitsanalyse die korrekte Funktion der durch die Konfiguration betroffenen Sicherheitsfunktionen unter Einbeziehung der physikalischen Prozessmodelle.
- Evaluierung der Ansätze zur Modellierung und Konsistenzprüfung anhand des Beispielsystems eines Kondensators innerhalb einer Destillationskolonne.