Generische Negativszenarien in der Entwicklung kollaborativer cyber-physischer Systeme

Viktoria Stenkova, Marian Daun, Jennifer Brings
viktoria.stenkova, marian.daun, jennifer.brings@paluno.uni-due.de
Universität Duisburg-Essen

Thorsten Weyer
thorstenweyer@uni-koblenz.de
Universität Koblenz-Landau

1 Motivation und Problemstellung

Negativszenarien beschreiben beispielhafte Systemabläufe, die nicht gewünscht sind und somit zu Problemen und Gefahren bei der Benutzung des Systems führen können [1]. Die Betrachtung von Negativszenarien ist insbesondere in der Entwicklung von sicherheitskritischen Systemen von Bedeutung, wie bspw. eingebetteter oder cyber-physischer Systeme [1]. Gerade bei dieser Art von Systemen geht der Trend in Richtung einer stärkeren Vernetzung von Systemen untereinander, um Funktionalität zu ermöglichen, die nicht von einzelnen Systemen erreicht werden kann. Diese Systeme werden oft als kollaborative cyber-physische Systeme bezeichnet. Beispielsweise erlaubt es eine kooperative adaptive Fahrgeschwindigkeitsregelung Fahrzeugen, sich zu einer Kolonne zusammenzuschließen und so den Treibstoffverbrauch und die Straßenauslastung zu reduzieren [2]. Für solche kollaborativen cyber-physischen Systeme ergeben sich neue Herausforderungen bezogen auf die Identifikation und Spezifikation von Negativszenarien. Haupttreiber hierfür ist die Einbettung eines Systems in den Kontext. Im Zusammenspiel mit anderen Systemen formieren sich dynamische Systemverbünde. Durch die mannigfaltigen Möglichkeiten in der Zusammensetzung dieser Systemverbünde ergibt sich eine sehr große Anzahl zu berücksichtigender Negativszenarien.

2 Generische Negativszenarien

Generische Negativszenarien [3] fassen mehrere Negativszenarien zusammen und gruppieren durch die Nutzung von Abstraktionsmechanismen gleichartige Instanzen und Nachrichten, um die Lesbarkeit zu erhöhen und den Umfang der Spezifikation zu verringern. Abbildung 1 illustriert dieses Prinzip. Kollaborative cyber-physische Systeme agieren in dynamischen Systemverbünden, die sich aus den unterschiedlichsten anderen Systemen zusammensetzen. Dieser Vielzahl möglicher Konfigurationen [4] muss bei der Definition von Negativszenarien Rechnung getragen werden, da unerlaubtes Verhalten in jeder Konfiguration untersucht werden muss. Die Erstellung von generischen Negativszenarien erfolgt in fünf Schritten. Dabei ist das Vorgehen stark an generelle Praktiken im szenariobasierten Requirements Engineering und in der Identifikation von Negativszenarien angelehnt:

- Zuerst werden positive Hauptszenarien identifiziert. Diese beschreiben zunächst die kleinstmögliche Anzahl an Systemen innerhalb des Systemverbunds.
- Im zweiten Schritt erfolgt die Identifikation von klassischen Alternativszenarien aus jedem Hauptszenario, wie sie im szenariobasierten Requirements Engineering geläufig sind.
- Im dritten Schritt werden die klassischen Alternativszenarien unter Berücksichtigung der verschiedenen möglichen Ausprägungen des Systemver-

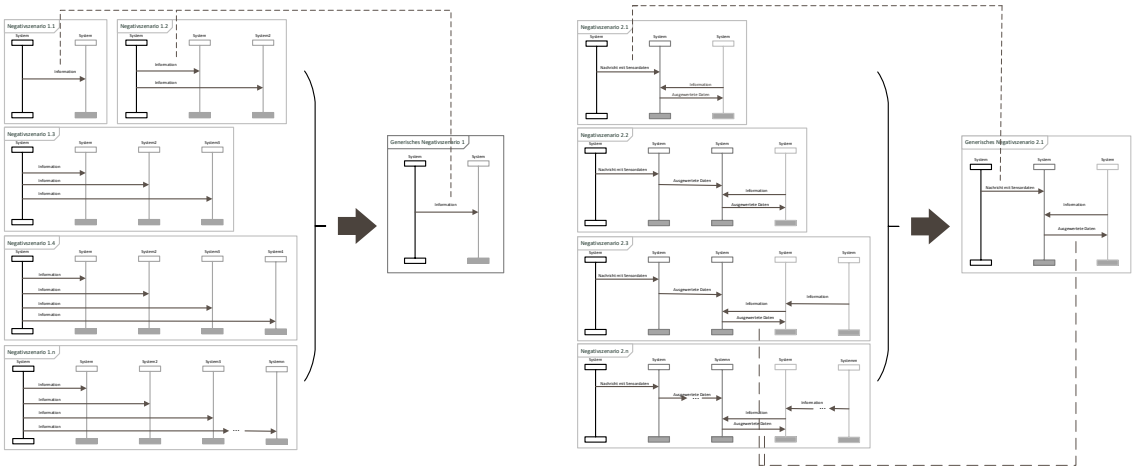

Abbildung 1: Zusammenfassung verhaltensähnlicher Negativszenarien zu generischen Negativszenarien

bunds exploriert. So entstehen alternative Konfigurationsszenarien mit einer unterschiedlich hohen Anzahl an abgebildeten Instanzen.

- Im vierten Schritt werden alle bisher erstellten Szenarien auf unerwünschtes Verhalten analysiert und zugehörige Negativszenarien definiert.
- Abschließend werden die generischen Negativszenarien erzeugt. Dies geschieht durch die Abstraktion eines gleichartigen Verhaltens verschiedener Systeme im Systemverbund.

3 Initiale Evaluation

Der vorgeschlagene Ansatz zur Spezifikation generischer Negativszenarien wurde bisher an einem industriellen Fallbeispiel evaluiert. Als Beispielsystem wurde eine kooperative adaptive Fahrgeschwindigkeitsregelung ausgewählt. Ausgehend von der vom Industriepartner zur Verfügung gestellten Spezifikation wurden Negativszenarien definiert und um mögliche Konfigurationen des Systemverbunds erweitert, woraufhin abschließend generische Negativszenarien abgeleitet wurden.

Die Evaluation am Fallbeispiel hat zunächst die Anwendbarkeit des Ansatzes bestätigt. Im weiteren Verlauf haben Diskussionen mit den Industriepartnern Indizien für die Nützlichkeit des Ansatzes aufgezeigt. Insbesondere scheint bei der Entwicklung kollaborativer cyber-physischer Systeme grundsätzlich die Notwendigkeit zu bestehen, durch zielgerichtete Abstraktion verschiedene Konfigurationen zusammenzufassen. Dies betrifft vor allem das Requirements Engineering, da eine fehlerhafte Nichtberücksichtigung von Systemverbundkonfigurationen auch eine Nichtidentifikation von wichtigen Anforderungen zur Folge haben kann. Eine Identifikation genauer Rahmenbedingungen und Einsatzzwecke dieses Mechanismus verbleibt jedoch zunächst für zukünftige Arbeiten.

Literatur

[1] S. S. Some. „Use Cases Based Requirements Validation with Scenarios“. In: *13th IEEE Int. Conf. on Requirements Engineering*. 2005, S. 465–466.

[2] D. Lu, Z. Li und D. Huang. „Platooning as a service of autonomous vehicles“. In: *A World of Wireless, Mobile and Multimedia Networks (WoWMoM), IEEE 18th Int. Symp. on*. 2017, S. 1–6.

[3] V. Stenkova, J. Brings, M. Daun u. a. „Generic Negative Scenarios for the Specification of Collaborative Cyber-Physical Systems“. In: *Conceptual Modeling - 38th International Conference, ER*. 2019, S. 412–419.

[4] J. Brings, M. Daun, T. Bandyszak u. a. „Model-based documentation of dynamicity constraints for collaborative cyber-physical system architectures: Findings from an industrial case study“. In: *Journal of Systems Architecture* 97 (2019), S. 153–167.