Modellierung und Analyse von Kommunikation in sicherheitskritischen Systemen basierend auf erweiterten Aufgabenmodellen

Tomasz Mistrzyk Gerd Szwillus

Abstract: Die Spezifikation und Analyse von Aufgabenmodellen bekommt eine besondere Bedeutung, wenn sicherheitskritische sozio-technische Systeme untersucht werden sollen. Eine außerordentliche Herausforderung stellt dabei die adäquate Abbildung der Kommunikation unter Berücksichtigung ihrer wichtigsten Parameter dar. In diesem Beitrag wird die Aufgabenmodellierungsumgebung AMBOSS zusammen mit den integrierten Konzepten von Barrieren, Topologie, Akteuren und insbesondere auch des Informationsflusses zwischen den einzelnen Aufgaben, vorgestellt. Zusätzlich werden die in AMBOSS integrierte Simulationsumgebung und deren Vorteile bei der Analyse von komplexen Systemen aufgezeigt. Abschliessend wird ein Rahmenwerk diskutiert, mit dem Kommunikation in Aufgabenmodellen auf deren Schwachstellen hin untersucht werden kann.

1 Einleitung

Bei der Betrachtung der Entwicklung sozio-technischer Systeme fällt auf, dass deren Komplexität auf mehreren Ebenen eine kontinuierliche Zunahme verzeichnet. Daraus resultieren auch stark wachsende Anforderungen an die Analyse solcher Systeme; auch die korrekte Gestaltung solcher Systeme stellt eine wachsende Herausforderung dar. Eine Schlüsselposition nimmt dabei die Kommunikation ein, die für eine adäquate Koordination der Aufgaben in einem sozio-technischen System verantwortlich ist. Kommunikationsfehler wurden bereits in der Fachliteratur als Hauptursache für kritische Ereignisse oder Unfälle identifiziert, was durch zahlreiche Beispiele untermauert wurde. Hierarchische Aufgabenmodelle repräsentieren einen etablierten Ansatz zur Abbildung der Aufgabenabhängigkeiten eines Systems. In diesen Modellen werden die Hauptaufgaben unter Berücksichtigung der temporären Relationen in ihre Unteraufgaben zerlegt. Es entsteht eine baumartige Struktur deren Hierarchietiefe von der Granularität der Aufgaben abhängig ist. Die Granularität steigt dabei proportional zu der gestrebten Hierarchietiefe. Aufgabenmodelle werden zur Unterstützung der Systementwicklung in frühen Phasen oder zur Dokumentation der Aufgabenanalyse eingesetzt. Darüber hinaus wurden Aufgabenmodelle bereits vielfach erfolgreich bei der Entwicklung von Benutzungsschnittstellen verwendet.

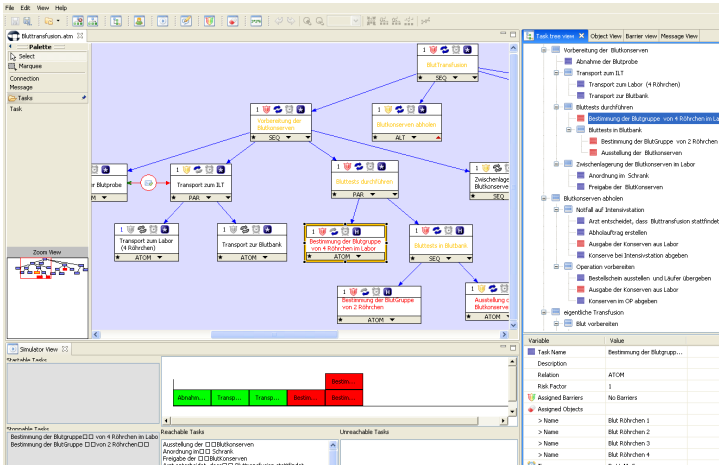

Abbildung 1: Die Modellierungsumgebung AMBOSS

2 Die Aufgabenmodellierungs- und Simulationsumgebung AMBOSS

Bisher existierende Aufgabenmodelle besitzen nur begrenzte Möglichkeiten die Aufgabenumgebung geeignet darzustellen; insbesondere werden wichtige Einflussfaktoren wie zum Beispiel Kommunikation bis jetzt nur marginal betrachtet. Dies ist ein erheblicher Nachteil, da – wie bereits erwähnt – fehlerbehaftete Kommunikation nachgewiesenermaßen in sicherheitskritischen Systemen eine häufige Ursache für kritische Zwischenfälle und Unfälle ist.

In der Modellierungsumgebung AMBOSS ist es nun möglich für jeden Informationsaustausch zwischen Unteraufgaben die beteiligten Akteure, also Sender und Empfänger von Nachrichten, zu spezifizieren. Es wird in einem Modell eindeutig festgehalten, welcher Akteur zu welcher Zeit welche Information versandt oder empfangen hat. Zusätzlich zu der Beschreibung des Informationsflusses werden die Information selbst, sowie das verwendete Übertragungsmedium, hinsichtlich der Übertragungssicherheit bewertet. So stehen dem Modellierer praxisnahe Kontrollstrukturen, die recht intuitiv genutzt werden können, wie etwa **Kontrollobjekte**, die die Nachrichtenübermittlung begleiten, **Feedbackkanäle**, die den Empfang einer Nachricht quittieren, oder **Protokolle**, die die korrekte Übertragung einer Nachricht sicherstellen zur Verfügung.

Amboss schließt mit seiner Simulationsumgebung für Aufgabenmodelle eine Lücke bisheriger Ansätze. In dieser Modellierungsumgebung können Einflussfaktoren im Zusammenspiel mit sicherheitskritischen Aspekten untersucht werden. Die Wechselwirkungen der einzelnen Parameter lassen sich interaktiv während der Simulation betrachten. Damit ist der Benutzer in der Lage, für eine bestimmte Aufgabe während der Simulation weitere Parameter gleichzeitig zu untersuchen. AMBOSS bietet ein Konzept von Sichten mit Hilfe dessen auf verschiedenen Abstraktionsebenen in einem erweiterten Aufgabenmodell sicherheitsrelevante Faktoren wie Topologie, Objekte und Barrieren, die mit Aufgaben

verknüpft und von diesen manipuliert werden, zu untersuchen.

In die Modellierungsumgebung wurden unter anderem die topologischen Eigenschaften der Aufgaben integriert. Dank dieses Konzeptes ist es möglich eine Aussage über die Zugehörigkeit zwischen Aufgaben und Objekten in Räumen zu treffen. Das Konzept der **Topologie** erlaubt Räume zusammen mit deren Eigenschaften zu kreieren, um die Abhängigkeit zwischen Aufgaben und der räumlichen Situation, in der Aufgaben ausgeführt werden, zu modellieren. Ein weiteres Konzept, das in AMBOSS aufgenommen wurde, ist das Konzept der **Barrieren**. Barrieren werden als spezielle Art von Objekten modelliert; sie haben eine Schutzfunktion, indem sie zwischen der Gefahr und dem zu schützenden Bereich installiert werden. Aufgaben können Barrieren je nach Situation aktivieren oder deaktivieren, d.h. ihre Schutzfunktion einschalten bzw. abstellen. Darüber hinaus können jeder Aufgabe maximale, minimale und typische Zeitangaben zugewiesen werden; diese werden dann in der Aufgabenhierarchie von unten nach oben aufsummiert.

Dem Benutzer wird insgesamt ermöglicht, in einer flexiblen Umgebung durch unterschiedliche Sichten das Modell zu gestalten und zu analysieren. Da die Software unter dem Gesichtspunkt der Analyse komplexer Systeme entstanden ist, lag besonderes Augenmerk darauf, große Modelle relativ einfach darstellbar und die Bedienung intuitiv erlernbar zu gestalten. AMBOSS ist frei verfügbar und kann von den Seiten der Fachgruppe heruntergeladen werden:

`http://wwwcs.uni-paderborn.de/cs/ag-szwillus/lehre/ws05_06/PG/PGAMBOSS/index.php`

Basierend auf der oben vorgestellten Modellierungsumgebung für sicherheitskritische Systeme entstand in Rahmen der Dissertation von Mistrzyk ein Rahmenwerk mit dem die Kommunikation in Aufgabenmodellen auf deren Schwachstellen untersucht wird. Die Methodologie besteht aus vier Schritten, die dem Experten Abweichungen (wie auch latente Fehler) in der Kommunikation zwischen den kommunizierenden Einheiten (Aufgabe + Rolle) aufzuspüren erlauben. Nach der Erstellung eines vollständigen Aufgabenmodells kommt es zu einer Klassifikation der einzelnen Kommunikationsvorgänge. In diesem Schritt kann herauskristallisiert werden welche Vorgänge während der Kommunikation besonders kritisch sind (oder waren). Danach werden in einem Top-Down Vorgehen die vorher festgelegten Eigenschaften der Kommunikation aus der Sicht des Senders und Empfängers untersucht. Dieser Schritt beinhaltet vor allem die binäre Beurteilung der Parameter. Anhand dieser Ergebnisse kann eine tiefergehende Analyse erfolgen, in der eine qualitative Abschätzung der Parameter durchgeführt wird. Die Ergebnisse werden akkumuliert und in einer geeigneten Form dargestellt. An dieser Stelle kann entschieden werden, wo sich das schwächste Glied der Kommunikation befindet, was für Ursachen es dafür gibt, aber auch was für Möglichkeiten zur Verfügung stehen diese Schwächen systematisch zu verbessern. Dieses Konzept hilft dem Experten ein strukturiertes Vorgehen anzuwenden, um mögliche Muster der Schwachpunkte in einem sicherheitskritischen System zu finden und diese Schritt für Schritt zu beseitigen.