Modellbasierte Risikoanalyse sicherheitskritischer Systeme

Erfahrungen mit einem UML-Profil im bahntechnischen Umfeld

Markus Schacher, KnowGravity Inc.

Die Europäische Norm für den Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit von Bahnanwendungen definiert Sicherheit als "Freiheit von für Menschen oder die Umwelt nicht akzeptierbaren Risiken" und Risiko als die "Kombination aus der erwarteten Häufigkeit eines Verlustes und der erwarteten Schwere dieses Verlustes". Dieser Artikel zeigt auf, wie sich solche Risikoüberlegungen in Form eines UML-Modells erarbeiten lassen.

Risiken im Bahnumfeld

Der Betrieb einer Eisenbahn birgt schon aufgrund der hohen Zahl der transportierten Passagiere ein inhärentes Betriebsrisiko. Sowohl technisches als auch menschliches Versagen kann zu fatalen Unfällen führen, die hohe Sachschäden verursachen oder gar Menschenleben gefährden können. Aus diesem Grund hat sich im Bahnumfeld über viele Jahrzehnte eine Sicherheitskultur entwickelt, die heute in Form der europäischen CENELEC-Norm [EN50126] niedergeschrieben ist. In dieser Norm sind nicht nur Techniken zur Identifikation und Begrenzung von Risiken beschrieben, sondern es wird auch das grundsätzliche Zusammenspiel zwischen Bahnbetreiber dessen Lieferanten geregelt.

Zentrales Konzept ist die Gefährdung: Eine Situation, die zu einem Unfall führen kann, aber nicht unbedingt muss. Dies kann beispielsweise ein Signal sein, das auf Grün steht, obwohl sich auf dem dahinter liegenden Gleis ein Zug befindet. Eine Gefährdung bezieht sich immer auf einen spezifischen Systemkontext, beispielsweise das Signal sowie dessen dahinter stehende Steuerlogik (Stellwerk) inklusive weiterer Sensoren. Auf dieser Basis lassen sich nun Szenarien analysieren, die zu verschiedenen Unfällen führen könnten. Diese Analysetechnik wird auch als „Ereignisbaumanalyse“ (eng. Event Tree Analysis, ETA) bezeichnet.

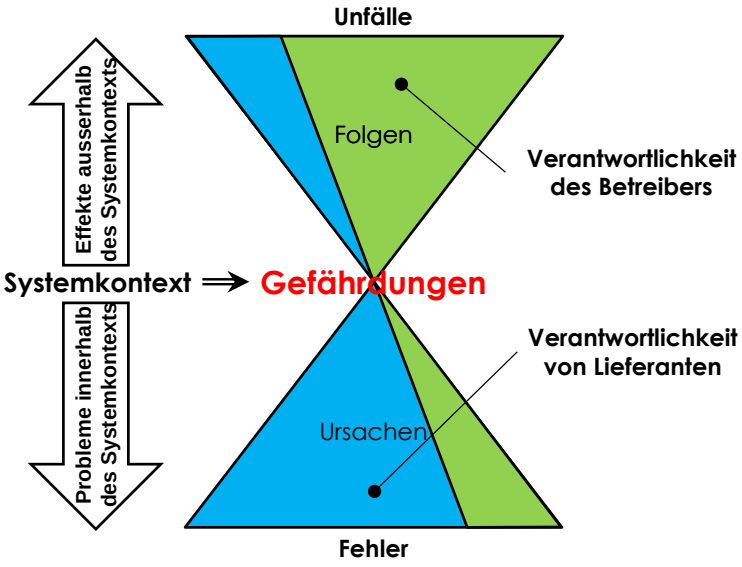

Abbildung 1: Ursachen und Folgen von Gefährdungen

Umgekehrt haben Gefährdungen auch immer Ursachen, die aus dem Inneren des Systemkontexts herrühren: Ein Sensor ist defekt, die Steuerlogik weist unter gewis-

sen Umständen fehlerhaftes Verhalten auf oder das Wartungspersonal hat eine fehlerhafte Konfiguration vorgenommen. Die Anwendung dieser Analysetechnik wird auch als „Fehlerbaumanalyse“ (eng. Fault Tree Analysis, FTA) bezeichnet.

Die Analyse der Folgen einer Gefährdung liegt nach EN50126 hauptsächlich in der Verantwortlichkeit des Bahnbetreibers: Er muss Zulassungsbehörden und damit der Öffentlichkeit gegenüber nachweisen, dass er mit den aus der Gefährdung resultierenden Risiken leben, d.h. mit ihnen umgehen kann. Dies kann er aber nur, wenn die Häufigkeit dieser Gefährdungen (die "Gefährdungsrate") ein gewisses Mass nicht überschreitet. Demgegenüber liegt die Verantwortlichkeit für die Analyse der Ursachen einer Gefährdung beim Lieferanten des Systems, welches durch den Systemkontext begrenzt ist. Er muss nachweisen, dass sein System die geforderte Gefährdungsrate unter keinen Umständen überschreitet. Für den Lieferanten sind also Gefährdungsraten sicherheitsrelevante Anforderungen, die er einhalten muss, um für sein System eine Zulassung zu erhalten.

Modellbasierte Risikoanalyse

Wird eine Risikoanalyse modellbasiert vorgenommen, so werden die wichtigen Konzepte der Risikoanalyse in Form von Modellelementen erfasst und zueinander in Beziehung gesetzt. Die wichtigsten Zusammenhänge zwischen diesen Konzepten sind in der folgenden Abbildung zusammengefasst:

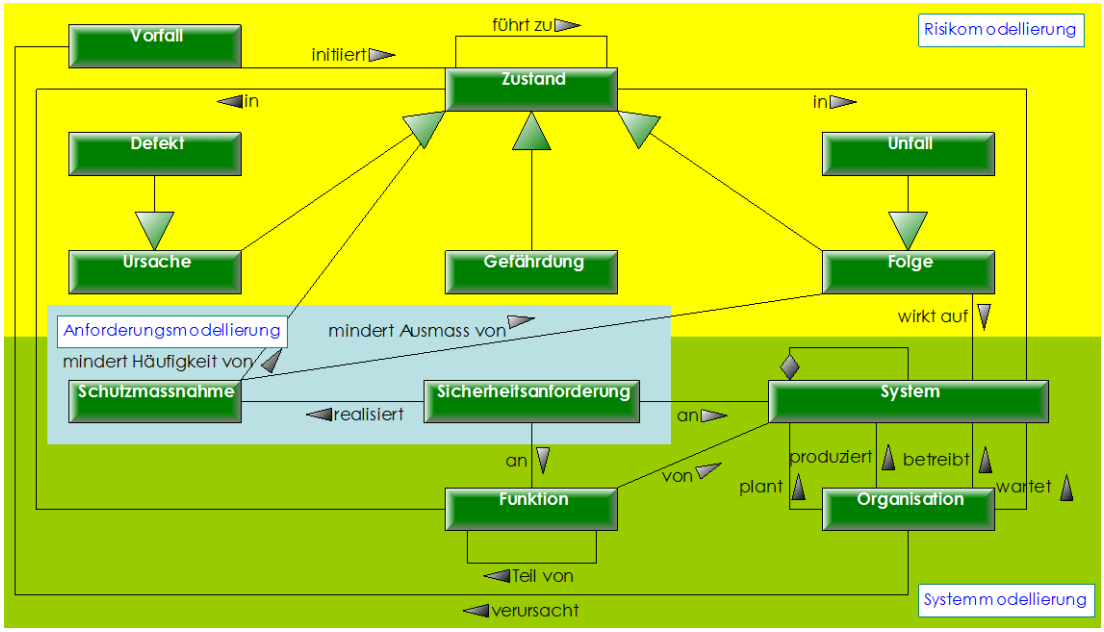

Abbildung 2: Konzepte einer Risikoanalyse

Thematisch lässt sich eine modellbasierte Risikoanalyse in drei Bereiche gruppieren:

- In der Systemmodellierung (grüner Bereich in Abbildung 2) werden die relevanten Systeme und Subsysteme sowie ihre Funktionen beschrieben. In detaillierter Form kann dies beispielsweise mittels der Systems Modeling Language [SysML] der OMG erfolgen. Zudem können in diesem Bereich verschiedene Organisationen als Systemverantwortliche festgelegt werden.
- In der Risikomodellierung (gelber Bereich) werden (System-)Zustände als Gefährdungen, Ursachen und Folgen klassifiziert, über Ursache/Wirkungs-

Beziehungen verknüpft sowie die auslösenden Vorfälle identifiziert. Diese Systemzustände lassen sich dann einzelnen Systemkomponenten (technische Modellierung) oder einzelnen Funktionen (funktionale Modellierung) zuordnen.

- Die Anforderungsmodellierung (blauer Bereich) verbindet die Systemmodellierung mit der Risikomodellierung, indem Schutzmassnahmen identifiziert werden, welche die Häufigkeiten unerwünschter Systemzustände minimieren und/oder deren Folgen reduzieren. Schutzmassnahmen werden dann mittels Sicherheitsanforderungen den ursächlichen Systemkomponenten bzw. Funktionen zugeordnet.

Risikoakzeptanz und Risikoevaluation

Eine für den Systembetreiber zentrale Technik ist die "Risikomatrix". Ein Risiko in der Risikomatrix ist eine mögliche Folge (typischerweise ein Unfall), die aus einer Gefährdung resultiert. Dazu werden die erwarteten Häufigkeiten der Folgen mit dem erwarteten Schadensausmass multipliziert und in die Risikomatrix eingetragen. Dies erlaubt die Klassifikation von Risiken bezüglich ihrer Häufigkeit (vertikale Achse) und ihrem Schadensausmass (horizontale Achse). Die beiden Achsen werden typischerweise in ein paar wenige sprechende Bereiche unterteilt.

Durch die Quantifizierung der Achsen lassen sich die den Zellen zugeordneten Risiken quantifizieren und deren Akzeptierbarkeit beurteilen (siehe Abbildung 3): Mit der Masseinheit "Geld pro Zeiteinheit" illustrieren diese Zahlen die jeweiligen Risiken sehr deutlich: dieser Betrag weist ein enormes Spektrum auf und ist jeweils pro angegebener Zeiteinheit durch den Betreiber "auf die Seite zu legen" um ein Risiko zu decken, welches der jeweiligen Zelle zugeordnet ist.

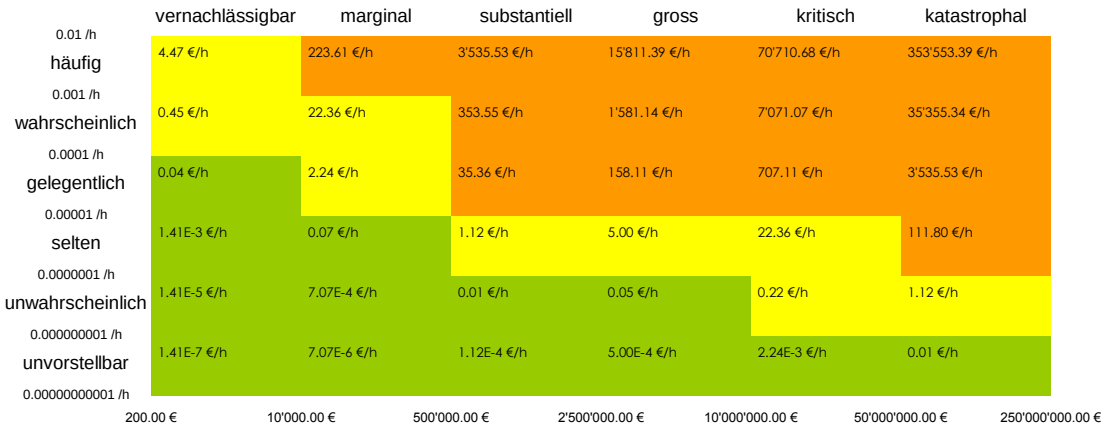

Abbildung 3: Risikoakzeptanz in der Risikomatrix

Typischerweise wird eine Risikomatrix in drei farblich getrennte Bereiche unterteilt:

- Die im grünen Bereich liegenden Risiken sind so klein, dass sie diskussionslos akzeptiert werden können.
- Die im roten Bereich liegenden Risiken sind so gross, dass sie keinesfalls akzeptiert werden können. Hier sind Massnahmen unumgänglich.
- Im gelben Bereich liegen Risiken, die Grenzfälle sind. Hier wird nur dann in Massnahmen investiert, wenn sie sich mit vernünftigem Aufwand realisieren lassen. Dieser Bereich wird auch "ALARP-Bereich" genannt ("As Low As Reasonably Practicable").

Das Ergebnis dieses Prozesses wird auch als "Risikoakzeptanz" bezeichnet, da es die Risikobereitschaft des Systembetreibers deklariert. Werden die einzelnen in der Risikoanalyse untersuchten Risiken in die Risikomatrix eingetragen, so wird dies als "Risikoevaluation" bezeichnet. Dies zeigt Abbildung 4 anhand dreier Risiken.

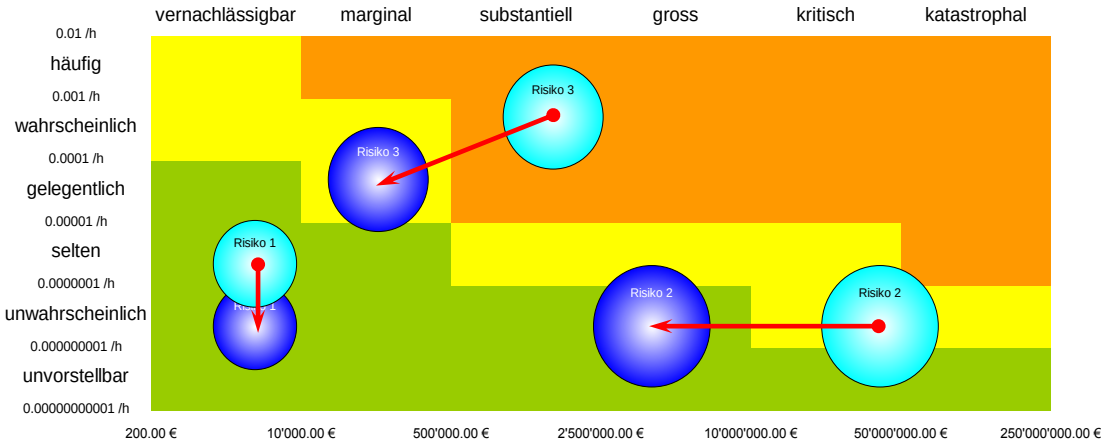

Abbildung 4: Risikoevaluation in der Risikomatrix

In der Abbildung ist jedes Risiko zweimal aufgezeigt: einmal ohne Berücksichtigung von Schutzmassnahmen (hellblau) und einmal mit deren Berücksichtigung (dunkelblau). Gegen Risiko 1 ist offenbar eine Schutzmassnahme zur Reduktion der Häufigkeit in Kraft. Demgegenüber wirkt bei Risiko 2 offenbar eine Schutzmassnahme zur Reduktion des Schadensausmasses. Bei Risiko 3 wirken offenbar beide Arten von Schutzmassnahmen sodass das Risiko vom inakzeptablen Bereich wenigstens in den ALARP-Bereich zu liegen kommt.

Domänenspezifische Modellierungssprachen mittels UML Profiling

UML Profiling ist ein Mechanismus, der schon seit über 10 Jahren Bestandteil der UML ist. Er erlaubt die Entwicklung domänenspezifischer Modellierungssprachen, die sich dann mit den meisten UML-Werkzeugen nutzen lassen. Ein UML-Profil ist ein spezielles Package, welches sogenannte Stereotypen definiert. Diese lassen sich auf Standard-Elemente der UML (wie Packages, Klassen, Anwendungsfälle, etc.) anwenden, um damit eine domänenspezifische Bedeutung auszudrücken. Ein Stereotyp kann zudem spezifische Eigenschaften für diese Modellelemente einführen (sogenannte „Tag Definitions“) und sogar ein eigenes Symbol besitzen.

Im Rahmen eines Projektes für die Schweizerischen Bundesbahnen haben wir nun ein UML-Profil für die Modellierung der wichtigen Konzepte aus Abbildung 2 entwickelt. Abbildung 3 zeigt einen Ausschnitt dieses Profils. Was in diesem Diagramm auffällt ist, dass die Namen vieler Tag Definitions mit einem Slash ("/") beginnen. Dies bedeutet, dass die Werte dieser Eigenschaften nicht durch den Modellierer festgelegt müssen, sondern durch das UML-Werkzeug automatisch berechnet werden. Dazu sind diesen Eigenschaften entspreche Formeln aus der Risikoanalyse hinterlegt.

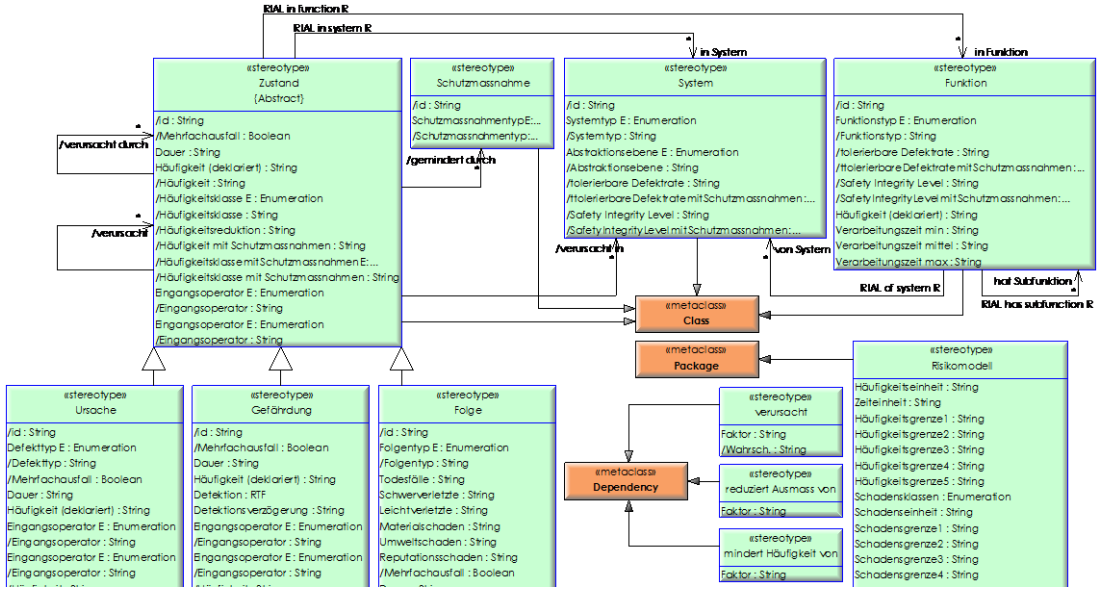

Abbildung 5: Ausschnitt aus dem UML-Profil für die Risikoanalyse

Anwendung

Abbildung 6 zeigt einen Ausschnitt aus einem vereinfachten Risikomodell für einen fiktiven Bahnübergang (die echten Risikomodelle sind wesentlich komplexer). Das Diagramm nutzt das oben eingeführte UML-Profil und zeigt sowohl Ursachen (gelb) als auch Gefährdungen (orange), die zu verschiedenen Kollisionen (rot) führen können. Die Kollisionen zeigen zudem einige der automatisch berechneten Eigenschaften mit und ohne Berücksichtigung von Schutzmassnahmen (grün) und Sicherheitsanforderungen (blau).

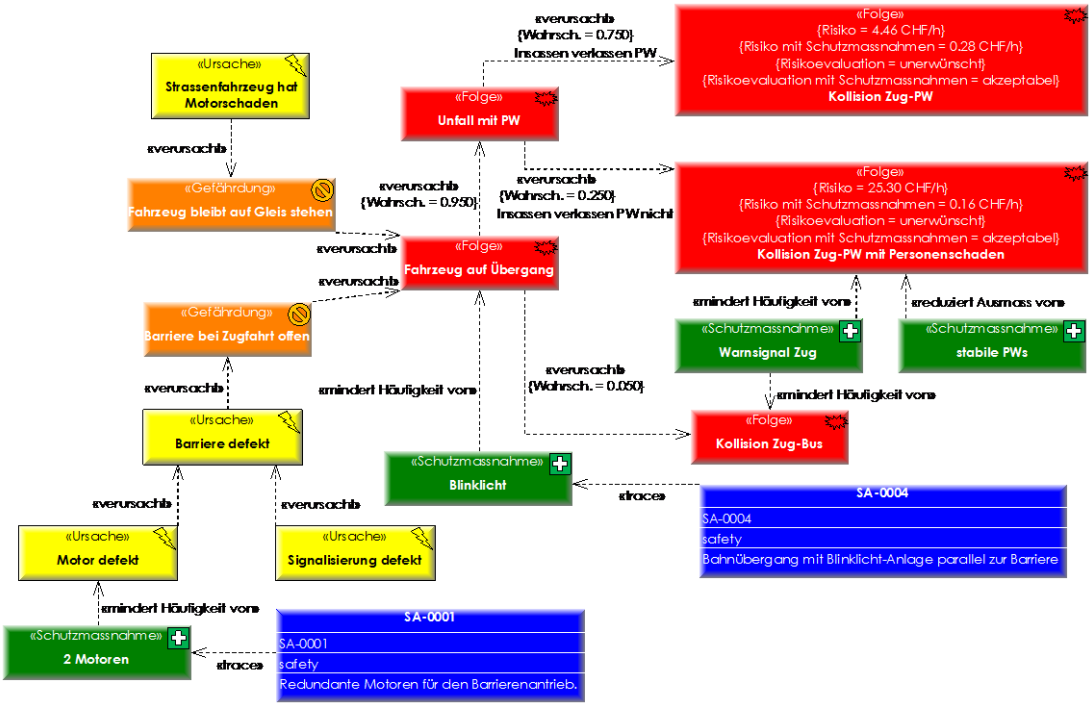

Abbildung 6: Ausschnitt Risikoanalyse "Bahnübergang"

Erfahrungen im praktischen Einsatz

Bei der projektspezifischen Ausarbeitung konkreter Risikoanalysen sind aber auch gewisse Schwierigkeiten aufgetreten:

- Kulturelle Schwierigkeiten: Nach mehr als 10 Jahren Stabilität wurden die EN 50126 Normen einer grösseren Revision unterzogen, die sich noch nicht etabliert hat. Dies führte bei Zulassungsbehörden und Bahnbetreiber zu unterschiedlichen Interpretationen und entsprechenden Diskussionen. Zudem war ein modellbasierter Ansatz für viele Beteiligten grundsätzlich neu, da Risikobetrachtungen bisher hauptsächlich mittels individueller EXCEL-Sheets durchgeführt wurden.
- Modell-Strukturierung: Es waren mehrere Iterationen notwendig, um eine optimale und gut wartbare Modellstruktur zu finden. Zudem war es oft schwierig, die Ursache für einen absurden berechneten Wert zu finden. Hier hat ein im Verlauf des Projekts eingeführter automatischer "Plausibilitäts-Check" grosse Erleichterung gebracht.
- Performanz: Die Client/Server-Architektur des verwendeten UML-Werkzeugs mit Client-seitigen Berechnungen war nur bedingt für die teilweise sehr komplexen Berechnungen geeignet. Dies führte dazu, dass die Diagramm-Editoren teilweise sehr träge auf Änderungen reagierten, da viele Eigenschaften neu durchgerechnet werden mussten.

Zusammenfassung

Die Risiken komplexer, heterogener Systeme können und müssen quantifiziert werden, damit sie nachvollziehbar, akzeptierbar und damit auch vertretbar gemacht werden können. Die modellbasierte Risikoanalyse ermöglicht eine strukturierte Identifikation von Systemrisiken sowie die systematische Ableitung von Gegenmassnahmen und Sicherheitsanforderungen aus diesen Risiken. Mittels UML Profiling lässt sich eine modellbasierte Risikoanalyse mit einem herkömmlichen UML-Werkzeug durchführen und bei Bedarf eng mit anderen Modellen verknüpfen. Der Autor ist auch in die Weiterentwicklung des UML Testing Profils [UTP] der OMG für modellbasiertes Testen involviert. Hier ist insbesondere die Integration von Risikoanalysen mit Techniken des risikobasierten Testens von grossem Interesse.

Literatur- und Quellenverzeichnis

[EN50126] CENELEC: Railway applications - The specification and demonstration of Reliability, Availability, Maintainability and Safety (RAMS) - Part 1: Generic RAMS Process, CENELEC - European Committee for Electrotechnical Standardization, WG14, prEN 50126-1, DRAFT, 04-SEP-2012

[SysML] Object Management Group: OMG Systems Modeling Language (OMG SysML™) – version 1.3, ptc/2012-06-01, Juni 2012

[UTP] Object Management Group: UML Testing Profile (UTP) – version 1.2, ptc/2012-09-13, September 2012

Autor

Markus Schacher ist Mitbegründer und KnowBody von KnowGravity Inc., einem kleinen aber feinem Beratungsunternehmen mit Sitz in Zürich (Schweiz), welches sich auf modellbasiertes Engineering spezialisiert hat. Als Trainer hat Markus bereits 1997 die ersten öffentlichen UML-Kurse in der Schweiz durchgeführt und hat als Berater vielen grossen Projekten geholfen modellbasierte Techniken einzuführen und nutzbringend anzuwenden. Heute ist er als aktives Mitglied der Object Management Group (OMG) in die Entwicklung verschiedener Modellierungssprachen involviert und ist Ko-Autor dreier Bücher zu den Themen Geschäftsregeln, SysML sowie operationellen Risiken.

Kontakt

Internet: www.knowgravity.com
Email: markus.schacher@knowgravity.com