

Ein generisches Informationsmodell für durchgängige IT-Toolchains im Kontext des Model-Based Systems Engineering

Nicolae Cioroi¹, Oliver Bleisinger¹, Akram Mechergui¹,
Johannes Krautkremer¹, Sven Kleiner¹

¹:em engineering methods AG, Rheinstr. 97, 64295 Darmstadt

Keywords: *Model-Based Systems Engineering, Informationsmodell, IT-Toolchain, Traceability*

Zusammenfassung: Die effiziente Anwendung von MBSE setzt anforderungsgerechte IT-Toolchains für definierte Anwendungsfälle des Systems Engineering voraus. Zur Aufwandsreduktion und Qualitätssteigerung bei der Definition von IT-Toolchains wird im Forschungsprojekt CyberTech ein generisches Informationsmodell entwickelt, welches als Blaupause zur Konzeption spezifischer IT-Toolchains verwendet werden kann. Dieser Beitrag beschreibt exemplarisch die Verwendung des Informationsmodells für den MBSE Anwendungsfall *Model-Based Safety* und die daraus folgenden Vorteile wie Aufwandreduktion, systematische Definition der Anforderungen an Toolchains und Toolschnittstellen sowie Traceability-Konzepte. Zudem kann das präsentierte Informationsmodell als Grundlage für die zielgerichtete Diskussion zum Ist- und Soll-Zustand zu Entwicklungsprozessen und Methoden sowie unternehmensübergreifende Businessarchitekturen genutzt werden.

1 Einleitung

Die Entwicklung komplexer Systeme erfordert eine Zusammenarbeit diverser Engineering Disziplinen und den Einsatz unterschiedlicher IT-Tools zur Erstellung und Pflege von Entwicklungsartefakten. Dabei ist es entscheidend, eine nahtlose Verbindung (*Seamless Traceability*) von Informationen zwischen IT-Tools sicherzustellen, um eine ganzheitliche Betrachtung des Systems sowie die Zusammenarbeit beteiligter Disziplinen zu verbessern. Für eine effektive Umsetzung von Model-Based Systems Engineering (MBSE) sind in der Praxis daher durchgängige IT-Toolchains notwendig. Für die Auswahl der richtigen Tools für einen oder mehrere MBSE Anwendungsfälle sowie der Sicherstellung der *Traceability* der Engineering Artefakte, ist ein gutes Verständnis der MBSE Methodik und ein erheblicher zeitlicher sowie finanzieller Aufwand notwendig. Zur Aufwandreduktion und gleichzeitiger Qualitätssteigerung bei der Definition von IT-Toolchains wird im Rahmen des CyberTech Forschungsprojekts [1] ein generisches und umfassendes Informationsmodell erstellt, das als Vorlage bzw. Blaupause genutzt werden kann. Das Informationsmodell beschreibt die wesentlichen Domänen von Systems Engineering im Allgemeinen, ohne sich auf bestimmte IT-Toolchains oder unternehmensspezifische Lösungen einzuschränken.

Der Stand der Technik zeigt, dass aktuell keine ganzheitlichen Modelle oder Beschreibungen von IT-Toolchains existieren, die alle wesentlichen Entwicklungsartefakte beinhalten. Ziel dieses Beitrags ist es den Aufbau und die exemplarische Anwendung eines generischen Informationsmodells zu demonstrieren. Als Fallbeispiel dient der Aufbau einer Toolchain für den MBSE Anwendungsfall *Model-Based Safety Analysis* im Bereich Medizintechnik, welche auf früheren Erkenntnissen des Forschungsprojekts CyberTech bezüglich der funktionalen Dekomposition [2] basiert. Weitere Anwendungsfälle des Informationsmodells werden in diesem Beitrag ebenfalls gelistet sowie abschließend Implikationen und Empfehlungen für zukünftige Forschungsarbeiten auf diesem Gebiet vorgestellt.

2 Stand der Technik und Wissenschaft

Der aktuelle Stand der Technik und Wissenschaft zu Informationsmodellen im MBSE als Grundlage für *Seamless Traceability* zwischen SE-Artefakten und Toolchains wird durch verschiedene Vorarbeiten geprägt. Es wurde bereits eine MBSE-Ontologie vorgestellt, die sieben Hauptbereiche für die wichtigsten Aspekte und Konzepte der Systementwicklung beinhaltet [3]. Die sieben Hauptbereiche decken dabei system-, bedarfs-, architektur-, lebenszyklus-, prozess-, kompetenz- und projektbezogene Konzepte ab. Ein Schwerpunkt liegt dabei auf den systembezogenen Konzepten, die grundlegende Prinzipien im Zusammenhang mit Systemen, Systems-of-Systems und Teilsystemen abdecken. In weiteren Arbeiten wurden demgegenüber Aspekte im Bereich Stakeholder Requirement Definition, Requirement Analysis, Operational and Maintenance Process, Verification Process und des Risk Management Process betrachtet [4]. Die Arbeiten im Kontext des Forschungsprojekts BaSysPLM fokussieren sich wiederum nur auf die Beschreibung eines durchgängigen Informationsmodells für Produktstrukturen, wie sie im Produktdatenmanagement bekannt sind, sowie der Durchgängigkeit von Entwicklungsartefakten, die für die Produktion notwendig sind [5]. In weiteren Quellen ist ein Prozess zur Erfüllung von Compliance-Anforderungen im Systems Engineering und Projektmanagement beschrieben, der die Nutzung eines Datenarchitektur-Frameworks [6] und die Implementierung von Model-Based Systems Engineering (MBSE) ermöglicht. Das Datenarchitektur-Framework berücksichtigt die Entwicklung von Systemarchitekturen für System-of-Systems (SoS) und Einzelsystemen zur Durchführung von Analysen sowie der Verifikation und Validierung. Der Prozess und das Datenarchitektur-Framework berücksichtigen auch die Verwaltung von Produkten im Lebenszyklus und die Integration von Stakeholdern auf verschiedenen Architekturebenen. Obwohl die genannten Informationsmodelle wichtige Aspekte der Entwicklung abbilden sind diese oft auf bestimmte Themen wie die funktionale Sicht oder das Variantenmanagement fokussiert. Es fehlt jedoch ein übergreifendes Informationsmodell, das alle relevanten Aspekte und Artefakte abdeckt um eine Seamless Traceability zu ermöglichen. Hierdurch würde die holistische und durchgängige Nachverfolgbarkeit von Zusammenhängen zwischen domänenspezifischen Entwicklungsartefakten durch die gesamte Toolchain auf eine nahtlose Weise ermöglicht. In neueren Publikationen im Bereich des System Lifecycle Managements [7, 8] wird zwar die Notwendigkeit eines generischen Datenmodells hervorgehoben, jedoch keine konkrete Umsetzung für durchgängige IT-Toolchains im MBSE präsentiert. Die Nutzung eines solchen Informationsmodells unterstützt die Durchgängigkeit zwischen Domänenartefakten im MBSE und verbessert somit die Entwicklung komplexer Systeme.

3 Konzept des generischen Informationsmodells

Das generische Informationsmodell ist in folgende sieben Domänen unterteilt: *Configuration Management*, *System Domain*, *Discipline-Specific Domain*, *Safety Domain*, *Simulation*, *Change Management* sowie der *Verification & Validation Domain*. Im Modell werden nur übergeordnete, toolneutrale Artefakte der jeweiligen Domänen gelistet. Untermengen an spezifischeren Artefakten können definiert werden, sind allerdings nicht relevant für die generische Darstellung der Verlinkungen zwischen den jeweiligen Domänen, sondern Teil des Tailorings. Die hier dargestellten Artefakte sollen generisch genug sein, um unabhängig von der Branche und Größe eines Unternehmens als Blaupause für IT-Toolchains zu dienen.

Die Entwicklungsartefakte im Modell sind mittels Kompositions-, Aggregations- oder Assoziationsbeziehungen verlinkt. Die Assoziationsbeziehungen besitzen eine Bezeichnung des Beziehungstyps sowie einen Pfeil mit Richtungsangabe. Beispielsweise ist *Technical Element* mittels *realizes*-Beziehung mit dem *Logical Element* verknüpft (Bild 1). Für alle Beziehungen ist die Multiplizität der Elemente definiert. Im vorherigen Beispiel beträgt die Multiplizität von *Logical Element* zu *Technical Element 1..n* zu *0..1*. Dies bedeutet, dass ein oder mehrere logische Elemente von maximal einem technischen Element realisiert werden können. Jedes technische Element soll mindestens ein logisches Element repräsentieren. In Bild 1 werden die *System*, *Discipline-Specific* und *Safety Domain* exemplarisch dargestellt, da diese im Fallbeispiel für *Model-Based Safety Analysis* genutzt werden (Abschnitt 5).

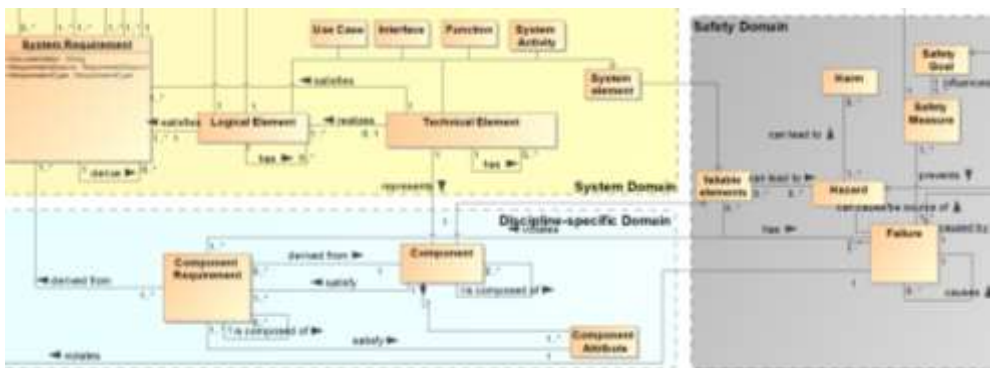


Bild 1: Darstellung der Verlinkungen zwischen *System Domain*, *Safety Domain* und *Discipline-Specific Domain* des generischen Informationsmodells

Wie in Bild 1 dargestellt, existieren domänenübergreifende Links zwischen Artefakten der *System Domain* und *Discipline-Specific Domain*. Beispielsweise führt von *Component Requirement* ein *derived from* Link zu *System Requirement*. *Component Requirement* ist seinerseits über einen *satisfy*-Link mit dem zentralen Element *Component* in der *Discipline-Specific Domain* verlinkt. Das Artefakt *Failure* in der *Safety Domain* kann mit mehreren *Component Requirements* assoziiert sein. Das Artefakt *Failable Elements* aus der *Safety Domain* kann eins der folgenden Artefakte der *System Domain* sein: *Use Case*, *System Activity*, *Function*, *Logical Element*, *Interface*, *Technical Element*. *Failable Elements* kann eine Beziehung zu *Failure* besitzen. *Component* repräsentiert das Systemartefakt *Technical*

Element und ist per *represents* verlinkt. Ein *Component* in der *Discipline-Specific Domain* kann z.B. CAD-Bauteil, Software-Klasse, Simulationskomponente oder elektrisches Kabel sein. Attribute einer *Component* können beim CAD Bauteil einzelne Flächen oder bei einer Software-Klasse einzelne Code-Begriffe sein. Ein *Component* kann wiederum aus weiteren *Components* bestehen und kann, ebenso wie ein *Technical Element*, ein reales Bauteil repräsentieren dem eine Sachnummer zugewiesen werden kann.

4 Anwendung und Tailoring des generischen Informationsmodells

Anhand eines Fallbeispiels aus der Medizintechnik, einer FMEA (Fehlermöglichkeits- und Einflussanalyse) für ein Beatmungsgerät, wurde ein erstes Tailoring des generischen Informationsmodells vorgenommen. Das Fallbeispiel greift den MBSE Anwendungsfall *Model-Based Safety Analysis* auf und nutzt das generische Informationsmodell, um eine IT-Toolchain sowie die Verlinkung notwendiger Artefakte (Datenobjekte) für eine FMEA darzustellen. Nachfolgend wird nicht die Durchführung einer FMEA oder Vorstellung der Architektur des Beatmungsgerätes thematisiert, sondern ein Einblick in die Verwendung bzw. das Tailoring des generischen Informationsmodells dargestellt.

Aus dem generischen Informationsmodell muss für den gewählten MBSE Anwendungsfall ein spezifisches Informationsmodell für die Definition und Umsetzung der IT-Toolchain entwickelt werden. Das generische Informationsmodell unterstützt die Definition des spezifischen Modells durch die Bereitstellung der generischen Elemente, die ein oder mehreren äquivalenten Elementen in der spezifischen Toolchain besitzen können. Somit wird einerseits der Aufwand für die Konzeption und Entwicklung der FMEA Toolchain reduziert und andererseits sichergestellt, dass die wichtigsten Artefakte für die Durchgängigkeit zwischen den Tools berücksichtigt werden. Ein vollständiges Verständnis welche Artefakte miteinander verlinkt sein sollen und in welchen Tools die sich befinden, hilft Fehler wie das Ausrollen von Tools ohne nahtlosen Datenaustausch oder eine falsche Aufwandabschätzung für die Toolchain Umsetzung vorzubeugen.

Das generische und daraus abgeleitete spezifische Informationsmodell kann außerdem als Grundlage für die systematische Erhebung von Toolanforderungen und zur Unterstützung einer Toolauswahl genutzt werden, falls diese noch nicht erfolgt ist. Für die *Model-Based Safety Analysis* Toolchain, wurden im Forschungsprojekt einige Tools bereits vorgegeben:

- Systemmodellierung (*System Domain*) – Cameo Systems Modeler
- Requirements Engineering (*System Domain*) – Siemens Polarion Requirements
- FMEA-Durchführung (*Safety Domain*) – Cameo Systems Modeler
- CAD Tool (*Discipline-Specific Domain: Mechanic*) – Siemens NX

Unter Berücksichtigung der vorgegebenen Tools können für die generischen Elemente nun spezifische Elemente und deren Verknüpfungen identifiziert werden. Dies erfolgt durch Analyse der Tools in der Anwendung, Analyse der vorgesehenen Entwicklungsmethode oder Befragung des Toolherstellers. Bild 2 zeigt rechts (dunkler Hintergrund) einen Ausschnitt des spezifischen Informationsmodells. Die durchgestrichenen Verbindungen (auch durch

<<abstraction>> gekennzeichnet) zeigen die dazugehörigen abstrakten Elemente des generischen Informationsmodells auf der linken Seite. Beispielsweise wird das generische *Component*-Artefakt im Tool für die Mechanik-Domäne für das Beatmungsgerät durch eine CAD *Assembly* oder ein *Part* repräsentiert.

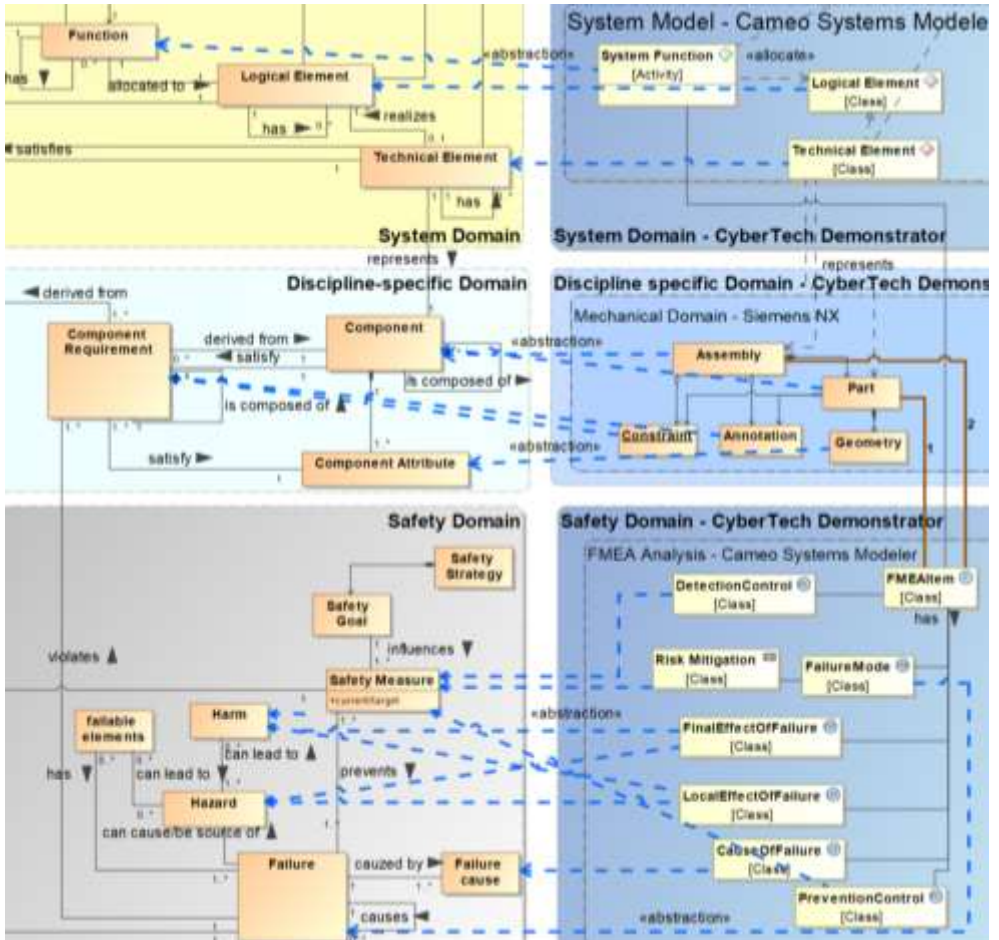


Bild 2: Zuordnung der spezifischen Engineering Artefakte für den *Model-Based Safety Analysis* Anwendungsfall (rechts) zu den Artefakten aus dem generischen Informationsmodell (links)

Im dargestellten Auszug des spezifischen Informationsmodells sind wichtige Verknüpfungen zwischen Artefakten in unterschiedlichen Tools, beispielsweise zwischen *FMEA Item* in Cameo und *Part* bzw. *Assembly* in Siemens NX mit Zahlen 1 und 2 im Bild 2 gekennzeichnet. Diese Verknüpfungen werden in der Praxis von der Entwicklungsmethodik vorausgesetzt.

Als Ergebnis haben IT-Verantwortliche und weitere Stakeholder einen klaren Überblick über die beteiligten Tools und Engineering Artefakte. Für die Verknüpfung der toolübergreifenden

Artefakte aus dem Cameo Systems Modeler und Siemens NX kann beispielsweise eine direkte Toolschnittstelle implementiert werden. Das spezifische Informationsmodell dient dann als Unterstützung zur Umsetzung der Toolchain, zur Definition konkreter Workflows sowie zur Softwarespezifikation bzw. Grundlage für die Schnittstellenentwicklung.

Mit einer direkten Schnittstelle oder einer alternativen IT-technischen Umsetzung für die Durchgängigkeit der Artefakte, können die *Components* und *Assemblies* aus Siemens NX direkt mit den FMEA Artefakten wie *FMEA Failure* in Cameo verknüpft werden. Zusätzlich können aus Siemens NX komponentenspezifische Anforderungen (in NX *Constraint* oder *Annotation*) wie Werte für Oberflächenrauheit oder Durchmesser von Bohrungen in Cameo für die FMEA Analyse bereitgestellt werden. Dadurch wird sichergestellt, dass keine Informationen zur Fehlersuche vergessen werden. Zudem kann nach einer Änderung der CAD-Elemente, die Auswirkung auf die FMEA direkt sichtbar dargestellt werden (*Impact Analysis* im MBSE).

Die Auswahl und Entwicklung der technischen Umsetzung der in den Informationsmodellen dargestellten Anforderungen für einen spezifischen MBSE Anwendungsfall, bildet somit die Grundlage für ein *Seamless Traceability* Konzept für die Entwicklungsartefakte. *Seamless Traceability* wird in diesem Kontext, als lückenlose Verknüpfung der Artefakte entlang der gesamten Toolchain durch die Tools jeder Domäne verstanden, wobei die betrachteten Artefakte direkt durch dynamische Verlinkung miteinander verknüpft sind. Ein weiterer Anwendungsfall für das spezifische und generische Informationsmodell ist die Nutzung der definierten Artefakten als In- und Output für Entwicklungsmethoden und -prozesse sowie als Diskussionsgrundlage, welche Artefakte in welcher Form als Entwicklungsergebnis in dem jeweiligen Unternehmen schon erzeugt werden oder zukünftig erzeugt werden sollen.

5 Zusammenfassung und Ausblick

Im vorliegenden Beitrag wurde dargestellt, dass für die effiziente Nutzung von MBSE eine bedarfsgerechte IT-Toolchain benötigt wird. Die Definition solcher Toolchains bedingt einen hohen Zeit- und Kostenaufwand. Eine Herausforderung bildet die eindeutige Definition erzeugter Engineering Artefakte und deren Verlinkung zueinander. Eine weitere im Beitrag diskutierte Herausforderung liegt in der Definition der Anforderungen an die IT-Tools, deren Auswahl sowie Integration mit bereits im Unternehmen existierenden IT-Tools. Zur Lösung dieser Herausforderungen wurde in diesem Beitrag ein generisches Informationsmodell vorgestellt, das als Blaupause für die Definition der anwendungsfallspezifischen IT-Toolchains verwendet werden kann. Das generische Informationsmodell beinhaltet die wesentlichen Artefakte aus Systementwicklung in einer übergeordneten, toolneutralen Form.

Weiterhin wurde die exemplarische Anwendung des generischen Informationsmodells für den MBSE Anwendungsfall *Model-Based Safety Analysis* demonstriert. Die Hauptschritte sind die Definition eines spezifischen Informationsmodells basierend auf dem generischen Modell sowie die Berücksichtigung bestehender IT-Tools und relevanter Datenobjekte. Das Ergebnis dieses Tailorings kann zur Definition von Toolanforderungen, der weiteren Toolauswahl sowie der Ausdetaillierung eines Traceability-Konzepts genutzt werden.

Um sicherzustellen, dass der aktuelle Stand des generischen Informationsmodells eine ausreichende Detaillierungstiefe erreicht hat, sind vom Autorenteam weitere Maßnahmen und die Umsetzung eines komplexeren Demonstrators geplant. Im Rahmen des CyberTech Forschungsprojekts [1] soll eine erweiterte IT-Toolchain für mehrere Anwendungsfälle im MBSE, darunter *Model-Based Requirements Engineering*, *Model-Based Systems Architecting* und *Model-Based Safety Analysis* definiert werden.

Danksagung

Dieses Forschungs- und Entwicklungsprojekt wird durch das Bundesministerium für Bildung und Forschung (BMBF) im Programm „Innovationen für die Produktion, Dienstleistung und Arbeit von morgen“ - Richtlinie zur Förderung von Projekten zum Thema „Beherrschung der Komplexität soziotechnischer Systeme – Ein Beitrag zum Advanced Systems Engineering für die Wertschöpfung von morgen (PDA_ASE)“ gefördert. Die Arbeiten wurden im Rahmen des Verbundprojekts CyberTech gefördert (Förderkennzeichen 02J19B010) und vom Projektträger Karlsruhe (PTKA) betreut. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autorenteam.

Literaturverzeichnis

- [1] T. Steinbach, B. Schleich, M. Ćorić, „Leitbild und Status zum Advanced Systems Engineering für die Entwicklung von Cyber-Technischen Systemen“, system:ability, 2023.
- [2] J. Kaspar, N. Cioroi, M. Bauch et al., „Guidelines for systematic functional decomposition in model-based systems engineering“, IEEE International Symposium on Systems Engineering (ISSE), 2022, doi: 10.1109/ISSE54508.2022.10005482.
- [3] J. Holt, S. Perry, „SysML for Systems Engineering: A Model-Based Approach“, Computing and Networks, 2018, doi: 10.1049/PBPC020E.
- [4] L. C. van Ruijven, „Ontology for Systems Engineering as a base for MBSE“, INCOSE International Symposium, 2015, doi: 10.1002/j.2334-5837.2015.00061.x.
- [5] C. Muggeo, T. Psota, J. Napitupulu et al., „A Product Ontology in the Research Project BaSysPLM“, prostep ivip Symposium, 2021.
- [6] R. K. Crain, „MBSE without a Process-Based Data Architecture is just a random set of Characters“, IEEE Aerospace Conference, 2014, doi: 10.1109/AERO.2014.6836221.
- [7] O. Bleisinger, T. Psota, J. Masiar, „Killing the PLM Monolith - the Emergence of cloud-native System Lifecycle Management (SysLM)“, 2022, doi: 10.24406/publica-88.
- [8] M. Eigner, „System Lifecycle Management – Digitalisierung des Engineerings“, Springer Vieweg, 2021, doi: 10.1007/978-3-662-62183-7.