



SIGNAL+DRAHT

Rail Signalling and Telecommunication



berner & mattner
optimizing your development

- Hochwertige Schnittstellenspezifikationen durch SysML-Modellierung



Hochwertige Schnittstellenspezifikationen durch SysML-Modellierung

Thomas Lauscher / Christian Fischer / Thorsten Hiebenthal

In diesem Artikel wird eine Vorgehensweise vorgestellt, die ausgehend von einer groben Systemsicht in klar definierten Schritten zu einer detaillierten Schnittstellenspezifikation führt. Die Vorgehensweise wurde in vielen Fachgesprächen mit Bahntechnikexperten der Deutschen Bahn AG entwickelt und ist daher besonders gut geeignet, im komplexen Bahnumfeld qualitativ hochwertige Spezifikationen zu erzeugen. Die Vorgehensweise ist zum Standard im Projekt NeuPro der DB Netz AG geworden. In diesem Projekt zeigt sich, dass die Vorgehensweise durch seine klare Strukturierung auch für sehr große Vorhaben und entsprechend große Teams von Spezifizierern sehr gut einsetzbar ist.

1 Einleitung

Die Betreiber von Eisenbahnnetzen sehen sich zunehmend mit der Anforderung konfrontiert, von verschiedenen Herstellern zugelieferte Teilsysteme integrieren zu müssen. Dabei tritt das Problem auf, dass es derzeit für viele Schnittstellen

noch keine detaillierten Spezifikationen gibt, an denen sich die Hersteller orientieren könnten. Aus diesem Grund werden bisher in der Regel ganze Komplettsysteme an einen einzigen Anbieter vergeben.

Die DB Netz AG hat sich im Rahmen des Projekts NeuPro das Ziel gesetzt, durch die Vorgabe standardisierter Schnittstellenspezifikationen größere Flexibilität zu erreichen. Um dieses Ziel zu unterstützen, hat die Berner & Mattner Systemtechnik GmbH die in diesem Artikel vorgestellte Vorgehensweise zur Schnittstellenspezifikation entwickelt. Die Vorgehensweise basiert auf der Modellierung mit SysML (Systems Modeling Language) [1]. Sie startet mit einer einfachen Sicht auf das Gesamtsystem und geht dann in klar definierten Schritten einen modellbasierten und redundanzfreien Weg zur fertigen Schnittstellenspezifikation.

2 Die Herausforderung

Nach der traditionellen Vorgehensweise erfolgt in der Zusammenarbeit von

Bahnbetreiber und Hersteller ein klar definierter Übergang, der sich im V-Modell nach EN 50126 [2] zwischen den Phasen 4 und 5 des RAMS-Lebenszyklus (im Folgenden als CENELEC-Phasen bezeichnet) darstellen lässt (Bild 1). Die blau markierten Kästen bezeichnen Aktivitäten, die vom Bahnbetreiber ausgeführt werden und die gelb markierten solche, die zu den Aufgaben des Herstellers zählen.

Der Bahnbetreiber beschreibt in Form von Lastenheften (CENELEC-Phase 4), WAS das zu entwickelnde System leisten soll. Der Hersteller wiederum entwickelt in den CENELEC-Phasen 5 und 6 in mehreren Schritten Spezifikationen, in denen die Realisierung (WIE) beschrieben wird. Durch diese klassische Arbeitsteilung liegt die Verantwortung für die Funktion des Gesamtsystems, bestehend aus dem ESTW und den Feldelementen, beim Hersteller. Die Konsequenz dieses Vorgehens ist, dass die Interoperabilität der Teilsysteme durch den Hersteller sichergestellt werden muss. Für den Bahnbetreiber ergibt sich, dass das System nur als Gesamtsystem beschafft werden kann.

Um dies zukünftig flexibler zu gestalten, will die DB Netz AG die Spezifikation der Schnittstellen detaillieren und standardisieren. Hierfür werden von der DB Netz AG Schnittstellenspezifikationen für diejenigen Schnittstellen, für die Interoperabilität sichergestellt werden soll, erstellt. Dabei müssen Aufgaben übernommen werden, die bisher den Herstellern überlassen waren. Im rechten Teil von Bild 1 ist dieser Sachverhalt durch Kästen mit blau-gelbem Hintergrund dargestellt.

Auf der linken Seite des V-Modells sind dies zum Beispiel Überlegungen zu Architektur und Verteilung auf einzelne Teilsysteme (CENELEC-Phase 5). Vereinzelt müssen auch Vorgaben für die CENELEC-Phase 6 getroffen werden, zum Beispiel Vorgaben von konkreten elektrischen Strömen und Spannungen. Auf der rechten Seite des V-Modells wiederum ergeben sich zusätzliche Aufgaben für den Bahnbetreiber, die bisher bei

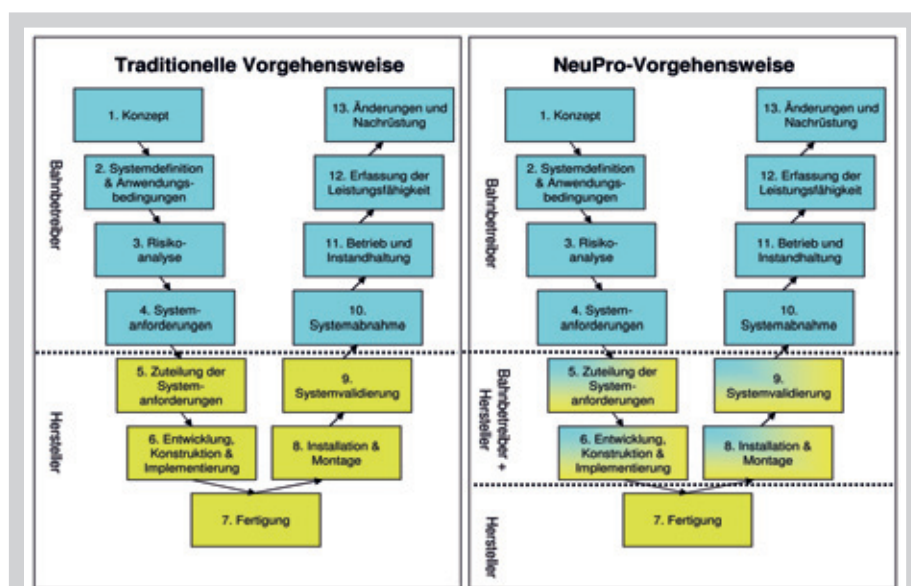


Bild 1: V-Modell nach EN 50126 mit alter oder neuer Vorgehensweise

den Herstellern in den GENELEC-Phasen 8 und 9 angesiedelt waren.

Das wichtigste Artefakt, das benötigt wird, um interoperable Systeme von verschiedenen Herstellern zu ermöglichen, ist die Schnittstellenspezifikation. Eine Schnittstellenspezifikation muss folgende Anforderungen umfassen:

- Sammlung und Darstellung aller funktionalen Abläufe, welche durch die Schnittstelle abgedeckt werden müssen.
- Sammlung aller nichtfunktionalen Anforderungen wie zum Beispiel RAMS(S)-Anforderungen, welche durch die Schnittstelle umgesetzt werden müssen.
- Detaillierung aller über die Schnittstelle zu übertragenden Daten sowie
- technische Details, die beachtet werden müssen, um zwei Teilsysteme miteinander verbinden zu können.

Die Anforderungen aus diesen Kategorien münden in eine technische Spezifikation der Schnittstelle über alle ISO/OSI-Ebenen.

Zu den Aufgaben des Erstellers einer Schnittstellenspezifikation gehört es, eine verbindliche Architektur vorzugeben, detailliert festzulegen, welche Aufgaben die einzelnen Teilsysteme besitzen und schließlich die Schnittstellen zwischen den Teilsystemen über alle ISO/OSI-Ebenen hinweg so präzise beschreiben, dass die Interoperabilität gewährleistet ist. Dies sind Aufgaben aus den GENELEC-Phasen 5 oder 6. Es handelt sich um Aufgaben, denen sich die Bahnbetreiber bisher so noch nicht stellen mussten.

Um den Anforderungen an die komplexe Tätigkeit des Schreibens von Schnittstellenspezifikationen gerecht werden zu können, ist eine kochrezeptartige Vorgehensweise wünschenswert, die die Fachleute für die Eisenbahntechnik durch alle notwendigen Schritte führt bis hin zur fertigen Schnittstellenspezifikation. Im Folgenden wird ein solcher Weg, der derzeit im Projekt NeuPro bei der DB Netz AG gegangen wird, beschrieben.

3 Der Lösungsweg

Der Lösungsweg ist in zwei Phasen aufgeteilt: Modellierung der fachlichen Ebene und Modellierung der technischen Ebene. Der Prozess der Schnittstellenmodellierung ist in dem Aktivitätsdiagramm in Bild 2 grafisch dargestellt.

Die fachliche Ebene ist eine funktionale, logische und abstrakte Sicht auf die Anforderungen, unabhängig von speziellen Lösungskonzepten. Lösungsbezo-

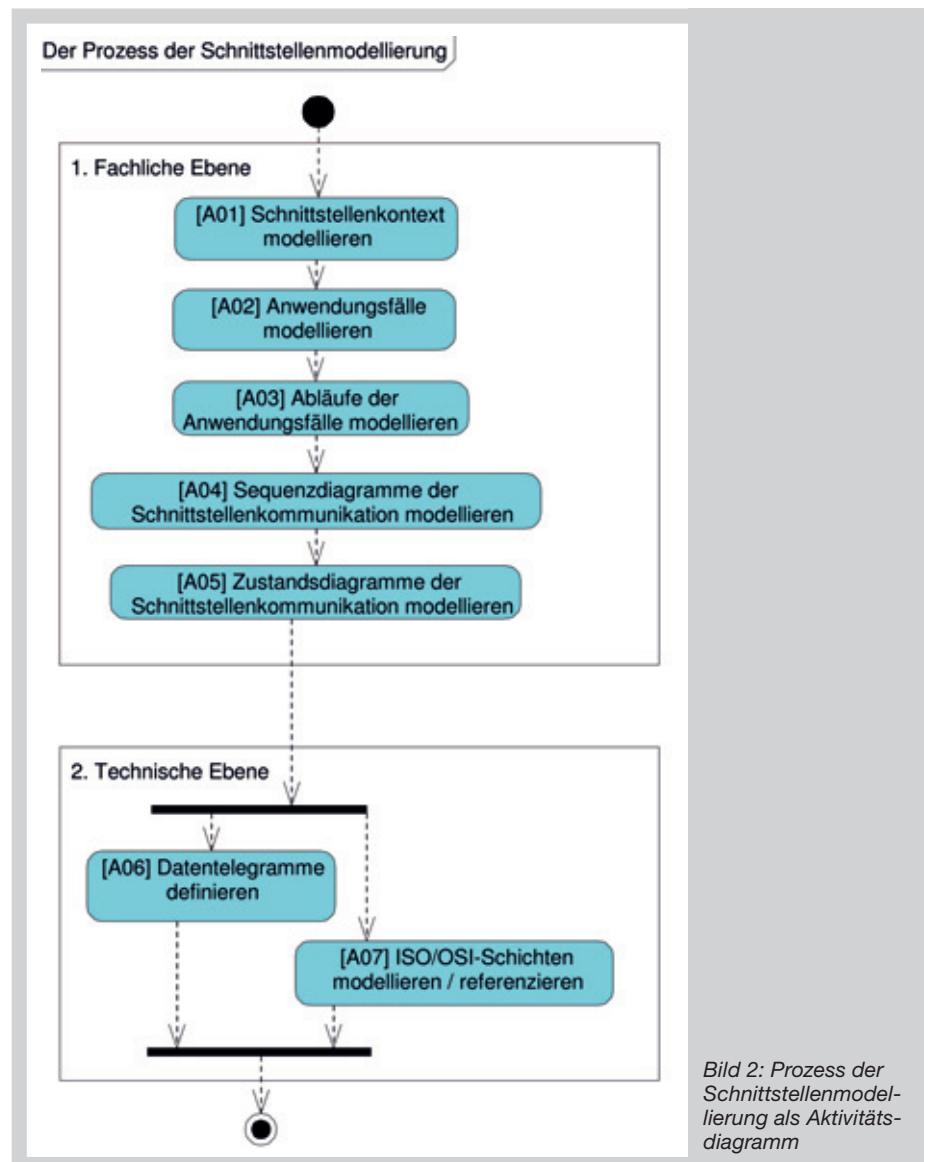


Bild 2: Prozess der Schnittstellenmodellierung als Aktivitätsdiagramm

gene Anforderungen wie physikalische, elektrotechnische oder softwaretechnische Beschreibungen werden in der technischen Ebene behandelt. Im Systems Engineering werden die Arbeiten an der fachlichen Ebene als Analyse-Phase bezeichnet.

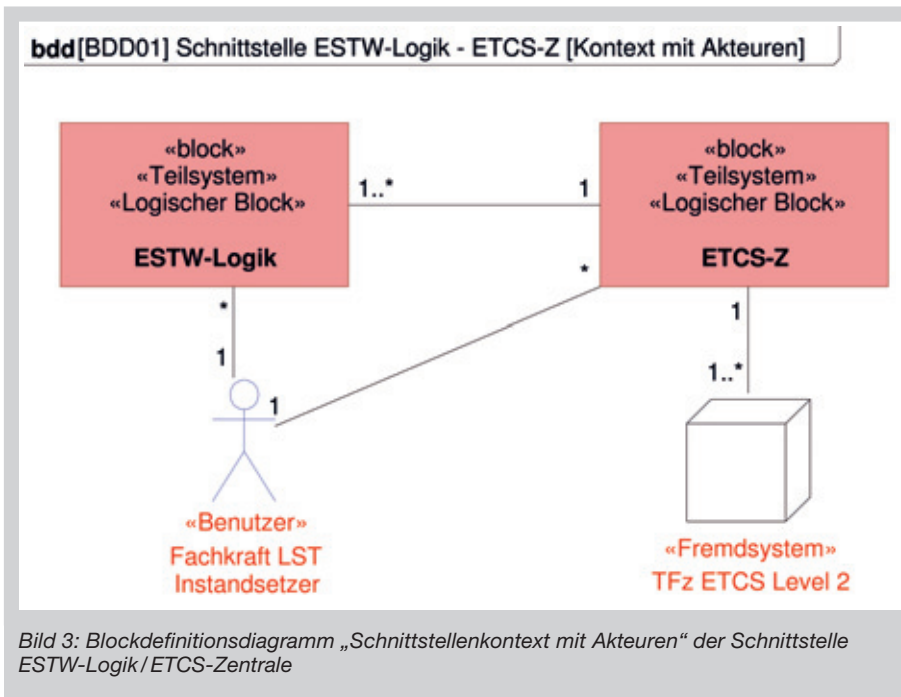
Die technische Ebene setzt die Anforderungen der fachlichen Ebene mit einem technischen Lösungskonzept um. Diese Phase wird im Systems Engineering als Design-Phase bezeichnet.

3.1 Aktivitäten auf der fachlichen Ebene

Zu Beginn muss festgestellt werden, welche Teilsysteme des Gesamtsystems Leit- und Sicherungstechnik an der Schnittstellenkommunikation beteiligt sind (im Folgenden als Schnittstellenendpunkte bezeichnet) und welche Teilsysteme bezüglich der zu spezifizierenden Schnittstelle eine Rolle spie-

len. Dies wird als der Schnittstellenkontext (also die Umgebung der Schnittstelle) bezeichnet. In der SysML kommt für diesen Zweck ein Blockdefinitionsdiagramm zum Einsatz. Es dient der Darstellung der statischen Struktur von Elementen (in SysML: Blöcken) und deren Beziehungen (in SysML: Assoziationen) untereinander.

Basis für die Definition einer Schnittstelle ist im Anschluss die Festlegung, welche Funktionalität auf welchem Teilsystem des Schnittstellenkontextes ausgeführt wird und welche dieser Funktionalitäten eine Kommunikation über die Schnittstelle erfordert. In der SysML geben Anwendungsfälle die Funktionalität eines Teilsystems in Form von Diensten, die ein Teilsystem für ein anderes Teilsystem oder eine menschliche Person anbietet (in der SysML als Akteure bezeichnet), wieder. Nach Festlegung des Schnittstellenkontextes müssen somit die für die Schnittstelle relevanten An-



wendungsfälle identifiziert und in einem Anwendungsfalldiagramm modelliert werden.

Ein Anwendungsfall setzt sich zusammen aus einem Ablauf von Aktionen, die in wechselnder Abfolge vom Akteur, der den Anwendungsfall nutzt, und von dem Teilsystem durchgeführt werden. Mit dem Aktivitätsdiagramm der SysML wird dieser Ablauf abwechselnder Akteur-Teilsystem-Aktionen modelliert. Es wird

im Detail festgelegt, welche Teilfunktionalität auf welchem Teilsystem in welcher Reihenfolge auszuführen ist.

Sind die Abläufe der Anwendungsfälle erarbeitet und ist die funktionale Verteilung auf die Teilsysteme fixiert, wird in einem nächsten Schritt innerhalb von Sequenzdiagrammen die Grundlage für die funktionale Spezifikation der Schnittstelle gelegt. Für Regelabläufe (erfolgreicher Standardablauf eines An-

wendungsfalls ohne Störungen) aus den erarbeiteten Aktivitätsdiagrammen wird die notwendige Kommunikation auf der Schnittstelle mit funktionalen Nachrichten (Kommandos und Meldungen) festgelegt.

Sequenzdiagramme eignen sich für die Darstellung der Interaktion einiger ausgewählter Kommunikationsszenarios. Da das Ziel eine möglichst vollständige Schnittstellenspezifikation sein muss, kommt nun ein neuer Diagrammtyp ins Spiel: Mit der Hilfe von Zustandsdiagrammen für die Teilsysteme der Schnittstellenendpunkte werden nun auch alle Ausnahmefälle erfasst und modelliert, sodass auf fachlicher Ebene ein hoher Grad an Vollständigkeit der Schnittstellenbeschreibung erreicht werden kann. Zuletzt bieten Zustandsdiagramme die Möglichkeit der Ausführung und Simulation, um eine weitergehende Optimierung und Tests der Anforderungen zu ermöglichen.

3.2 Aktivitäten auf der technischen Ebene

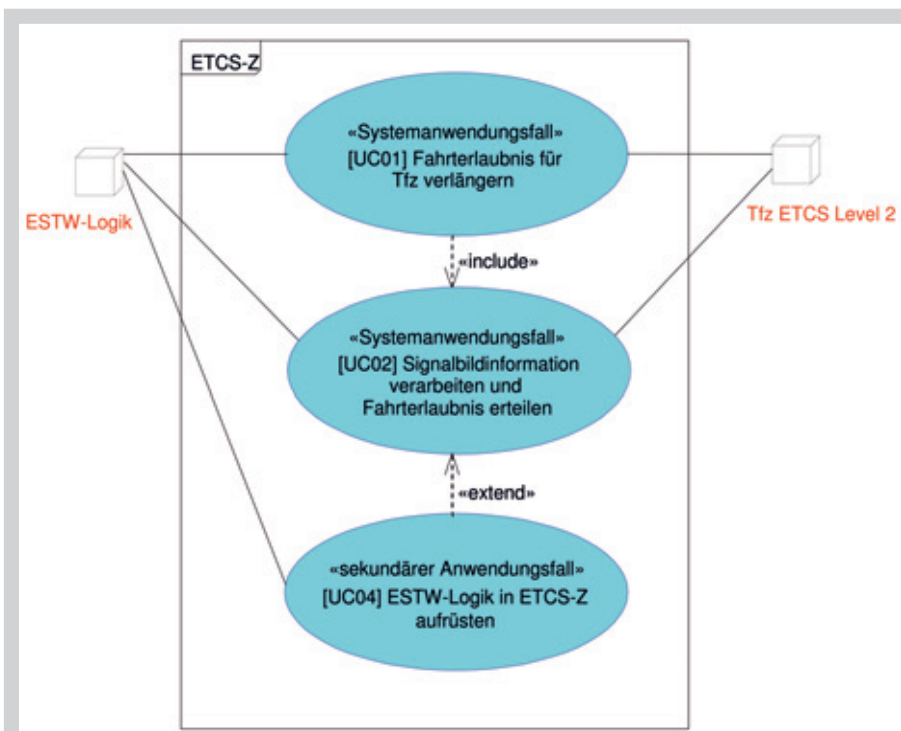
Den Abschluss der Schnittstellenspezifizierung bildet die Beschreibung der konkreten technischen Umsetzung. Dies beinhaltet zunächst die Beschreibung der ISO/OSI-Schichten (siehe Kapitel 8.1). Kommen Industrieprotokolle und -standards wie Ethernet und TCP/IP zum Einsatz, genügt ein Verweis auf deren Spezifikation. Zuletzt werden die technischen Datentelegramme inklusive der Beschreibung ihrer Bytes und Bits sowie ihre Wertebereiche und Bedeutungen definiert.

3.3 Der Berner&Mattner-SysML-Prozess, SYSMOD und OOSEM

Der in diesem Artikel vorgestellte Prozess zur Entwicklung von Schnittstellenspezifikationen ist Bestandteil eines umfassenden von der Berner & Mattner Systemtechnik GmbH entwickelten Prozesses zur Modellierung und Entwicklung von bahntechnischen Systemen mit SysML.

Der Gesamtprozess

- basiert auf den Vorgehensmodellen (Methodologien) SYSMOD (Systems Modeling Process) und OOSEM (Object-Oriented Systems Engineering Method),
- setzt das Konzept System of Systems (SoS) um,
- definiert eine Modellstruktur (umgesetzt durch SysML-Pakete),
- unterstützt die Modellierung von Varianten,



- integriert die Phasen des RAMS-Lebenszyklus [2],
- unterstützt drei Ebenen der Darstellung von bahntechnischen Anforderungen (betriebliche, fachliche und technische Ebene),
- erleichtert die Verständlichkeit durch Einschränkung der Anzahl der eingesetzten Modellelemente der SysML, Vorgabe von Modellierungsrichtlinien, Integration und Bevorzugung von bahntechnischen Termini und weitgehende Darstellung in deutscher Sprache.

Die in diesem Artikel beschriebene Modellierung der Schnittstellenspezifikation kann nahtlos und redundanzfrei in das Gesamt-SysML-Modell der Leit- und Sicherungstechnik eingegliedert werden. Die Modellierung der betrieblichen Ebene ist zur Erstellung von Schnittstellenspezifikationen nicht notwendig und wird daher an dieser Stelle nicht weiter behandelt.

Das dem Gesamtprozess zugrunde liegende Vorgehensmodell SYSMOD ist in der Literatur [3] von Tim Weilkiens, OOSEM in [4] von Sanford Friedenthal beschrieben worden. Beide beinhalten einen Weg mit SysML von den Top-Level-Anforderungen bis hin zur technischen Spezifikation. In den Vorgehensmodellen ist beschrieben, zu welchen Zeitpunkten im Prozess welcher Diagrammtyp der SysML in welcher Art und Weise einzusetzen ist und auf welche Art und Weise die verschiedenen Modellelemente verknüpft sind, damit Redundanz vermieden wird und Nachverfolgbarkeit gegeben ist.

4 Modellierung des Schnittstellenkontextes

Der Schnittstellenkontext wird innerhalb eines Blockdefinitionsdiagramms modelliert. Für das Beispiel der Schnittstelle zwischen der ESTW-Logik und der ETCS-Zentrale ist dieses Diagramm in Bild 3 dargestellt. Abgebildete Teilsysteme sind die ESTW-Logik, die ETCS-Zentrale (ETCS-Z) und zwei externe Akteure – ein ETCS-Level-2-geführtes Triebfahrzeug und eine „Fachkraft LST Instandsetzer“.

Zwischen der ESTW-Logik und der ETCS-Zentrale ist die zu beschreibende Schnittstelle als Assoziation dargestellt. Die ETCS-Zentrale besitzt eine Verbindung zu einem oder mehreren ETCS-Level-2-geführten Triebfahrzeugen. Der menschliche Akteur „Fachkraft LST Instandsetzer“ kann sowohl mit der ESTW-Logik als auch mit der ETCS-Zentrale kommunizieren.

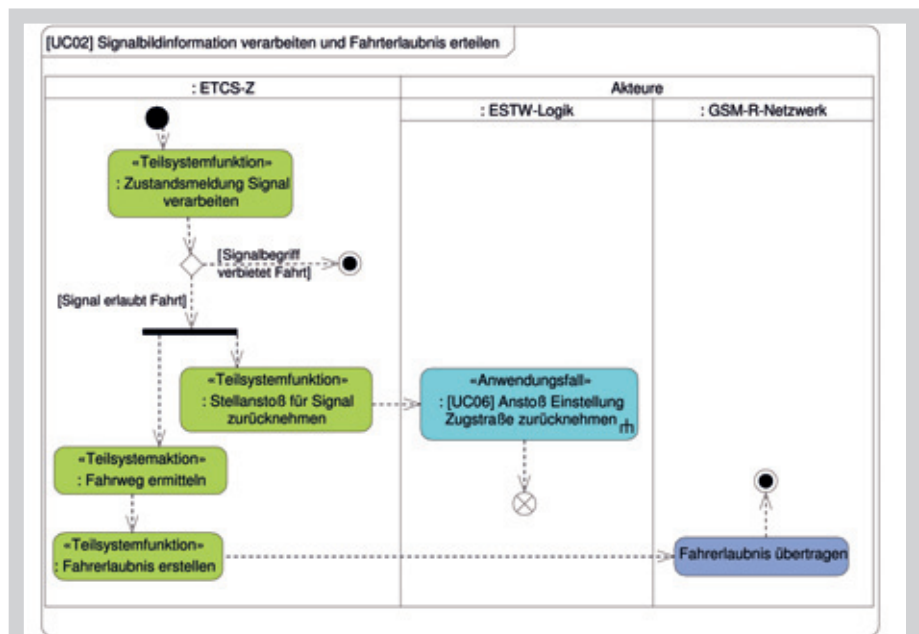


Bild 5: Aktivitätsdiagramm des Anwendungsfalls „Signalbildinformation verarbeiten und MA erteilen“ der ETCS-Zentrale

5 Anwendungsfallanalyse

Die Anwendungsfallanalyse ist ein unverzichtbarer Schritt auf dem Weg zu einer Schnittstellenspezifikation, auch wenn ihre direkten Ergebnisse, die Anwendungsfalldiagramme, nicht in jedem Fall in die Schnittstellenspezifikation aufgenommen werden. Meistens werden sie dann aufgenommen, wenn dem Leser einer solchen Spezifikation vermittelt werden soll, warum bestimmte Funktionalitäten auf der Schnittstelle stattfinden. In diesem Fall ergibt sich durch die Anwendungs-

falldiagramme eine lückenlose Nachvollziehbarkeit von den übergeordneten Anwendungsfällen bis zum letzten Bit auf der Schnittstelle. Wenn diese lückenlose Nachvollziehbarkeit nicht notwendig erscheint, werden die Anwendungsfalldiagramme in der Regel nicht in die Schnittstellenspezifikation übernommen.

Die Anwendungsfallanalyse wird nacheinander für jeden der beiden Schnittstellenendpunkte durchgeführt. Dabei wird jeweils die Frage gestellt, welche Dienste einer der Schnittstellenendpunkte für den jeweils anderen erbringen soll

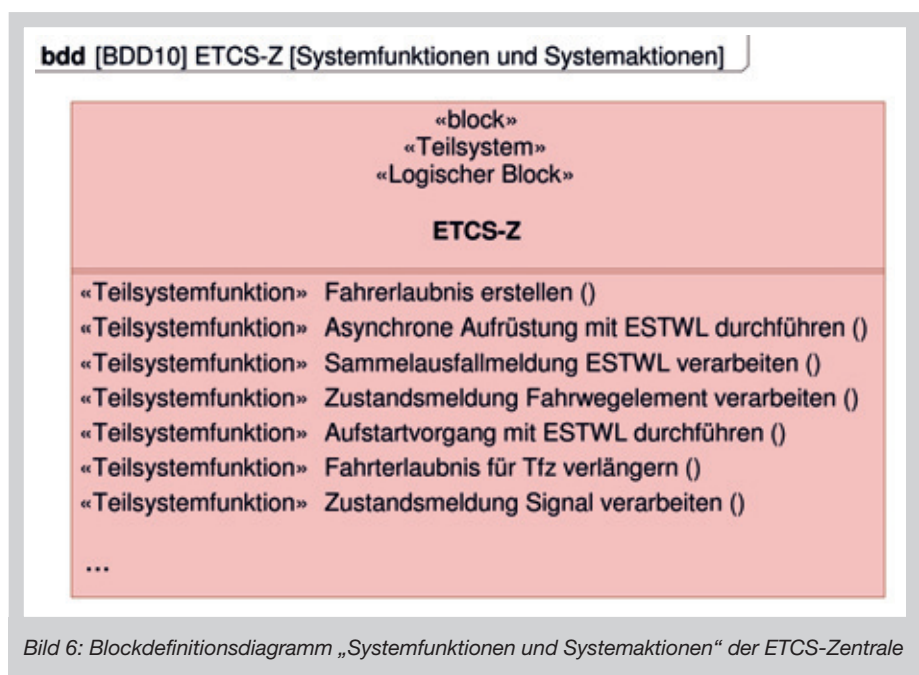


Bild 6: Blockdefinitionsdiagramm „Systemfunktionen und Systemaktionen“ der ETCS-Zentrale

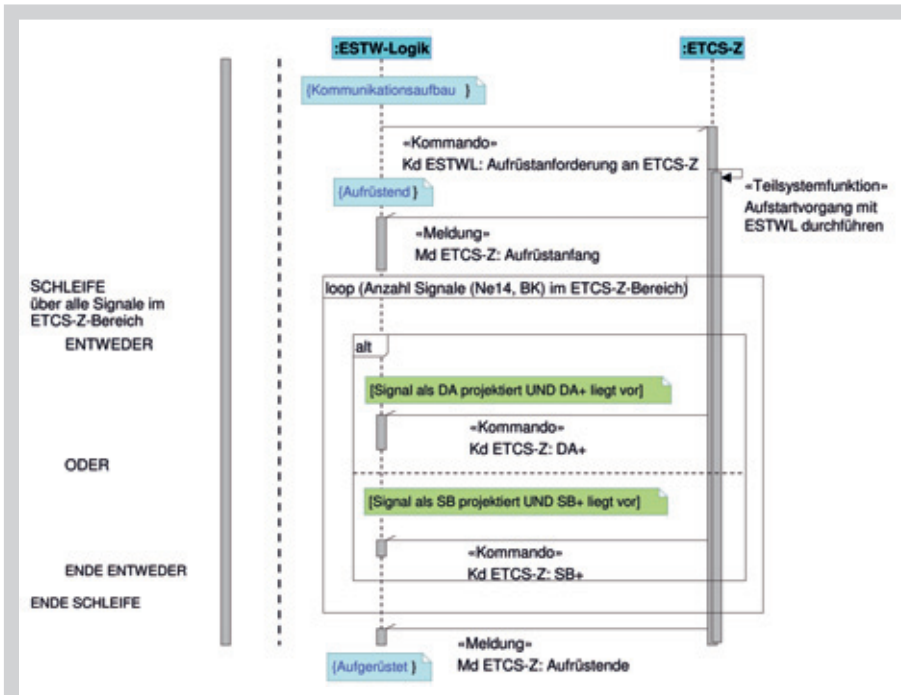


Bild 7: Sequenzdiagramm – Beispielszenario Aufrüsten der ESTW-Logik

und ob für einen Dienst eines Schnittstellenendpunkts eine Kommunikation über die Schnittstelle notwendig ist. Dadurch werden die Systemanwendungsfälle identifiziert. Systemanwendungsfälle stellen die tatsächlichen Anwenderziele eines Akteurs an den Schnittstellenendpunkt dar. Mit sekundären Anwen-

dungsfällen werden Ausnahmesituationen und wiederverwendete Teilfunktionalitäten der Systemanwendungsfälle modelliert.

Das Bild 4 zeigt als Beispiel denjenigen Teil der Anwendungsfälle des Teilsystems ETCS-Zentrale, die eine Verbindung zum Teilsystem ETCS-Zentrale besitzen,

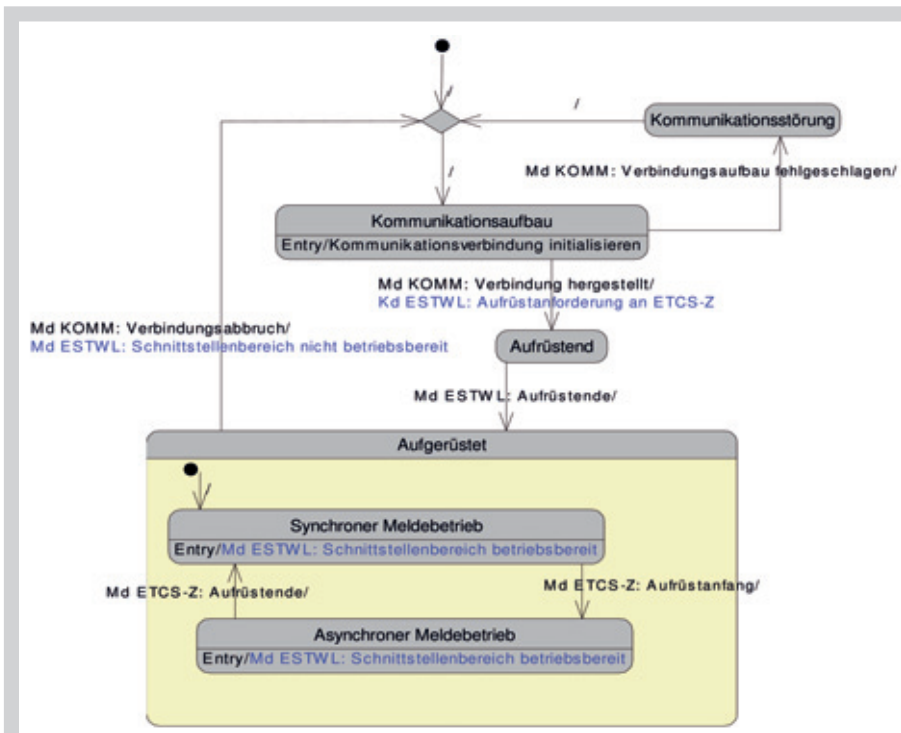


Bild 8: Zustandsdiagramm – Zustände eines Schnittstellenbereichs des Teilsystems ESTW-Logik

somit eine Schnittstellenkommunikation erfordern und schnittstellenrelevant sind. Das Diagramm enthält zwei Akteure, die von den Anwendungsfällen betroffen sind. Der sekundäre Anwendungsfall „ESTW-Logik in ETCS-Z aufrüsten“ ist durch eine „extend“-Beziehung mit dem primären Anwendungsfall „Fahrerlaubnis erteilen“ verbunden. Dadurch wird erkennbar, dass die Aufrüstung unter bestimmten Bedingungen (zum Beispiel nach Verbindungsabbrüchen) innerhalb des Anwendungsfalls UC04 zur Ausführung kommen kann. Der Anwendungsfall „Signalbildinformation verarbeiten und Fahrerlaubnis erteilen“ wird über die „include“-Beziehung vom Anwendungsfall UC01 eingebunden. Dies bedeutet, dass an einer bestimmten Stelle innerhalb des Ablaufs des Anwendungsfalls UC01 der Anwendungsfall UC02 ebenso zur Ausführung kommt.

6 Die Abläufe der Anwendungsfälle – funktionale Dekomposition der Schnittstellenendpunkte

Nach Durchführung der Anwendungsfallanalyse steht fest, welche schnittstellenrelevanten Aufgaben die beiden Teilsysteme der Schnittstellenendpunkte erbringen müssen. Noch ist nicht klar, welcher Ablauf sich hinter einem Anwendungsfall verbirgt und wie sich die einzelnen Schritte des Ablaufs eines Anwendungsfalls auf die beiden Schnittstellenendpunkte verteilen.

Um dies zu bestimmen, wird ein Aktivitätsdiagramm für jeden schnittstellenrelevanten Anwendungsfall gezeichnet, welches den gewünschten Ablauf des Anwendungsfalls abbildet. In Partitionen („Swimlanes“), welche die Teilsysteme der Schnittstelle darstellen, wird die funktionale Zuordnung der einzelnen Schritte (in der SysML als Aktionen bezeichnet) zur ETCS-Zentrale oder den Akteuren festgelegt. Der Arbeitsschritt, in dem diese Funktionsverteilung vorgenommen wird, wird als „funktionale Dekomposition“ bezeichnet.

Ist der allgemeine Ablauf und die Zuordnung zu den Teilsystemen festgelegt, wird das Aktivitätsdiagramm um zusätzliche Details erweitert. Eine Aktion, welche im Aktivitätsdiagramm eines Anwendungsfalls eines Teilsystems verwendet wird, kann nach der Definition von B&M einer der folgenden Typen sein:

- ein Aufruf eines anderen Anwendungsfalls,
- eine Teilsystemfunktion,
- eine Teilsystemaktion,
- eine einfache Aktion.

Eine Teilsystemfunktion ist so definiert, dass diese eine wesentliche, das Teilsystem beschreibende Funktion des Teilsystems von einer bestimmten Größe ist. Teilsystemaktionen hingegen sind kleinere Funktionen eines Teilsystems. Die Unterscheidung muss der Modellierer treffen. Sinn und Zweck der Unterteilung ist, die Liste der das Teilsystem beschreibenden Teilsystemfunktionen nicht mit kleinen und unwesentlichen Funktionen unnötig anwachsen zu lassen.

Eine einfache Aktion (in Bild 5 „Fahrerlaubnis übertragen“) kann in anderen Diagrammen nicht wiederverwendet werden. Ist eine Wiederverwendung gewünscht und handelt es sich nicht um eine Teilsystemfunktion, so ist die Aktion als Teilsystemaktion umzusetzen.

Ein Aufruf eines anderen Anwendungsfalls wird als Aufruf auf das Aktivitätsdiagramm des aufgerufenen Anwendungsfalls umgesetzt. Im Diagramm ist dies an der Forke rechts unten in der Aktion ersichtlich.

Eine Teilsystemfunktion und eine Teilsystemaktion werden als Aufruf einer SysML-Operation des Blocks des jeweiligen Teilsystems realisiert.

Auf die dargestellte Art und Weise unter Verwendung von Operationen und aufgerufenen Anwendungsfällen wird sichergestellt, dass die definierten Aktionen der Teilsysteme auch in folgenden Analyse- und Designschritten innerhalb von Sequenz- und Zustandsdiagrammen wiederverwendet werden können. Zusätzlich wird Redundanz vermieden. Dies führt zu einer konsistenteren und fehlerfreieren Spezifikation.

Diese Redundanzfreiheit und Konsistenz ist an dem folgenden Blockdefinitionsdiagramm (Bild 6) ersichtlich. Durch die Definition der Operationen eines Teilsystems innerhalb der Aktivitätsdiagramme sind diese nun zu Operationen des Blocks des Teilsystems geworden. Die Operationen können in allen folgenden Analyseschritten weiterverwendet und in diversen Ansichten dargestellt werden.

7 Modellierung der Kommunikation

Bis zu diesem Punkt wurden die Eigenschaften des Systems bestehend aus den beiden Schnittstellenendpunkten modelliert. Der nächste Schritt ist die Beschreibung der Kommunikation auf der Schnittstelle. Dazu gehören zum einen die konkreten Abläufe auf der Schnittstelle. Diese Abläufe werden in Form von Sequenzdiagrammen visualisiert.

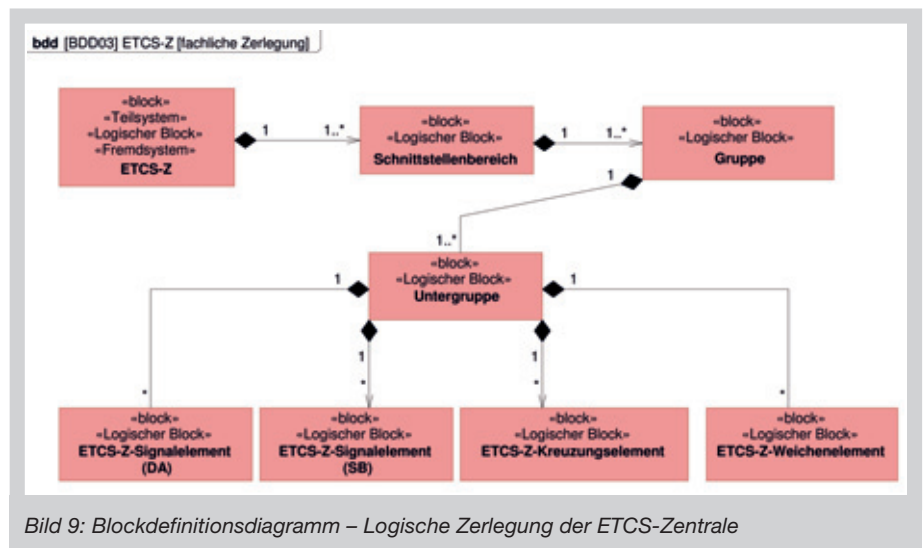


Bild 9: Blockdefinitionsdiagramm – Logische Zerlegung der ETCS-Zentrale

Weiterhin gehört zur Kommunikationsmodellierung die Reaktion der beiden Teilsysteme auf externe Stimuli, abhängig vom Zustand, in dem sich die Teilsysteme gerade befinden. Diese Sachverhalte werden in Form von Zustandsdiagrammen abgebildet.

7.1 Modellierung der Kommunikation – Sequenzdiagramme

In Sequenzdiagrammen wird zunächst das Regelverhalten auf der Schnittstelle beschrieben. Dabei wird in jedem Sequenzdiagramm jeweils genau ein Szenario dargestellt (Sequenz von Verarbeitungsschritten innerhalb eines Anwendungsfalls, die unter bestimmten Bedingungen auszuführen ist). Innerhalb eines Sequenzdiagramms sind zwar optionale Abläufe möglich, die Diagramme werden aber durch diese immer schwerer lesbar. Aus diesem Grund werden optionale Abläufe in der hier vorgestellten Vorgehensweise nur sehr sparsam eingesetzt. Für die Abbildung aller wichtigen Funktionalitäten, die von einer Schnittstelle unterstützt werden müssen, ist im Allgemeinen also eine ganze Reihe von Sequenzdiagrammen notwendig.

Das Bild 7 als Beispiel für ein Sequenzdiagramm zeigt die funktionalen Nachrichten, die zur Aufrüstung der ESTW-Logik durch die ETCS-Zentrale auf der Schnittstelle gesendet werden müssen. Diese Nachrichten lassen sich in Kommandos und Meldungen aufteilen. Diese funktionalen Nachrichten werden innerhalb des Modellierungswerkzeugs als Informationsobjekte definiert. Sie werden durchgängig benutzt, beginnend in den Sequenzdiagrammen, dann in der Folge in der Zustandsmodellierung und schließlich werden sie im technischen Teil durch konkrete Te-

legramminhalte festgelegt. Diese Vorgehensweise bietet den Vorteil, dass eine bestimmte Information, die über die Schnittstelle übertragen wird, immer gleich heißt – unabhängig davon, in welchem Diagrammtyp sie verwendet wird oder von welchem Modellierer sie modelliert wurde. Dadurch wird eine redundanzfreie Modellierung möglich, wodurch wiederum die Wiederverwendbarkeit von Modellelementen erleichtert wird.

Ein weiteres Merkmal der Sequenzdiagramme ist die Verwendung von Zustandsinvarianten (in Bild 7 gekennzeichnet durch hellblaue Rechtecke). Für diese werden Zustände aus den im folgenden Abschnitt behandelten Zustandsdiagrammen verwendet. Sie sorgen hier für ein erweitertes Verständnis der Systemzusammenhänge. Ein Zusammenhang zu den im Kapitel 6 dargestellten Teilsystemfunktionen ergibt sich durch die Modellierung von Operationsaufrufen, die als Reaktion auf empfangene Kommandos oder Meldungen ausgeführt werden.

7.2 Modellierung der Kommunikation – Zustandsdiagramme

In der Zustandsdiagrammmodellierung wird dargestellt, wie SysML-Blöcke auf Stimuli durch bestimmte Ereignisse reagieren, abhängig von dem Zustand, in dem sie sich gerade befinden. Im Allgemeinen können diese Blöcke komplette Systeme, Teilsysteme oder logische Komponenten sein. Im Rahmen der Schnittstellenspezifikationen in der Stellwerkstechnik werden Zustandsdiagramme für die Teilsysteme der beiden Schnittstellenendpunkte gezeichnet.

Das Bild 8 zeigt ein Beispiel für die Zustandsmodellierung des Schnittstellen-

Byte-Nr	Bit 7	Bit 6	Bit 5	Bit 4	Bit 3	Bit 2	Bit 1	Bit 0
1	Telegrammnummer 1234 (0x4D2)							
3	Transaktionsnummer							
5	L = Anzahl Zeichen im Text							
6	Text (ASCII, Byte 1 bis 40)							
6+L	Steuerbyte							
7+L	Sicherungsanhang							
Telegramminformation:								
Byte 1	Telegrammnummer (binär kodiert). Sie bezeichnet die Art des Telegrammes)							
Byte 3	Transaktionsnummer (binär kodiert). Diese Nummer identifiziert eindeutig eine Bedienhandlung und die zugehörige Bedienquittung.							
Byte 5	Anzahl Zeichen im Text (binär kodiert)							
Byte 6	Text (maximal 40 ASCII-Zeichen)							
Byte 6+L	Steuerbyte (binär kodiert) 0 = Textanzeige löschen 1 = Text anzeigen							
Byte 7+L	Sicherungsanhang – ein CRC über den vorhergehenden Telegramminhalt.							
Telegrammverwendungen:								
1. Kommando Text senden Steuerbyte = 1								
2. Kommando Text löschen Steuerbyte = 0								

Bild 10: Telegrammstruktur, Beschreibung der Telegrammfelder, Telegrammverwendungen

bereichs der ESTW-Logik. Der Schnittstellenbereich ist der Teil der ESTW-Logik, in dem alle benötigte Logik für die Kommunikation mit der ETCS-Zentrale enthalten ist. In dem Diagramm fällt zunächst auf, dass wie in den Sequenzdiagrammen Kommandos und Meldungen verwendet werden. Diese kommen sowohl als eingehende Ereignisse, auf die das System reagiert, vor (zum Beispiel die Meldung „Md Komm: Verbindung hergestellt“). Sie können aber auch ausgehende Ereignisse sein, die bei einem Zustandsübergang an das jeweils andere System gesendet werden (ein Beispiel hierzu ist das Kommando „Kd ESTWL: Aufrüstanforderung an ETCS-Z“, das beim Übergang in den Zustand „Aufrüstend“ gesendet wird).

Wichtig bei der Zustandsmodellierung für Schnittstellen ist, dass nicht versucht werden sollte, das komplette interne Verhalten der beiden Schnittstellenendpunkte zu modellieren. Vielmehr geht es darum, die für die Schnittstelle relevanten Teile zu identifizieren und für sie Zustandsmodelle anzufertigen. Für die Schnittstelle relevant sind jeweils diejenigen Zustände eines Systems, die entweder durch eingehende Informations-

objekte von der Schnittstelle beeinflusst werden oder selbst Informationen über die Schnittstelle versenden.

7.3 Logische Zerlegung eines Teilsystems

Im vorherigen Abschnitt wurde ein Zustandsdiagramm nicht für das gesamte Teilsystem des Schnittstellenendpunkts ESTW-Logik gezeichnet, sondern für einen Bestandteil der ESTW-Logik, einen Schnittstellenbereich. Die Tatsache, dass eine ESTW-Logik über mehrere Schnittstellenbereiche verfügt, ist der Grund, warum die Schnittstellenkommunikation nicht direkt im Zustandsdiagramm der ESTW-Logik angeordnet werden kann. Deshalb müssen teilweise im Rahmen der Schnittstellenspezifikation auch Bestandteile des Teilsystems definiert werden. Unterhalb eines Teilelements kann nun die Schnittstellenkommunikation als Zustandsdiagramm für ein einziges Teilelement modelliert werden.

Zusätzlich kann aus anderen Gründen die Notwendigkeit bestehen, das Teilsystem in logische Bestandteile zu zerlegen, um beispielsweise eine Zuordnung zu Funktionsgruppen zu realisieren oder um

die Zustandsdiagramme übersichtlicher, lesbarer und strukturierter zu gestalten. In Bild 9 wird das Teilsystem ETCS-Zentrale in logische Bestandteile aufgegliedert.

Es ist zu beachten, dass die logische Zerlegung nicht vollständig sein muss. Im Fall der Schnittstellenspezifikation würde dies sonst überflüssigen Zusatzaufwand generieren. Vielmehr wird empfohlen, lediglich diejenigen logischen Komponenten darzustellen, welche für die Schnittstellenspezifikation benötigt werden.

8 Vorgaben für die technische Umsetzung

Mit Abschluss der Zustandsdiagrammmodellierung sind der Aufbau und das schnittstellenrelevante Verhalten der betroffenen Teilsysteme vollständig dargestellt. Was nun noch fehlt, sind konkrete Vorgaben über die technische Realisierung. Eine herstellerübergreifende Interoperabilität bei einer Schnittstelle ist nur dann zu erreichen, wenn auch wichtige technische Details zwingend vorgegeben werden. Dabei sind Vorgaben zu machen, die zur technischen Lösung gehören und damit in den Verantwortungsbereich der Hersteller fallen. Dies ist notwendig, weil nur so verhindert werden kann, dass verschiedene Hersteller inkompatible Lösungen entwickeln.

In der Leit- und Sicherungstechnik, für die diese Vorgehensweise entwickelt wurde, werden fast ausschließlich telegrammbasierte Datenschnittstellen verwendet. Aus diesem Grund wird beispielhaft gezeigt, wie die Telegramme einer Schnittstelle so beschrieben werden können, dass kein Spielraum für unterschiedliche Interpretationen bleibt.

Das Bild 10 zeigt im oberen Teil einen beispielhaften Aufbau eines Daten-telegramms, das heißt seine Struktur in Bytes und Bits. Daran schließt sich im mittleren Teil eine Beschreibung sämtlicher Felder im Telegramm an. Schließlich wird im unteren Teil für jedes Vorkommen des Telegramms in einem Sequenz- oder Zustandsdiagramm eine sogenannte Telegrammverwendung festgehalten.

Mit dem Begriff Telegrammverwendung wird hier eine konkrete Verwendung eines Telegramms als Kommando oder Meldung bezeichnet. Die Definition der Telegrammverwendung beschreibt den Inhalt aller Felder, die die konkrete Verwendung als Kommando oder Meldung ausmachen. Im obigen Beispiel ist das nur das Steuerbyte, da dieses zwischen den beiden Telegrammverwendungen „Text senden“ und „Text

Nr	OSI-Schicht	Aufgaben	Protokollbeispiele
7	Anwendungen (Application)	- Verschafft Anwendungen Zugriff auf das Netzwerk	HTTP, FTP, HTTPS, SMTP, LDAP
6	Darstellung (Presentation)	- Datenumwandlung in einheitliche Darstellung für die Übertragung - Datenkompression - Datenverschlüsselung	
5	Sitzung (Session)	- Sitzungsverwaltung (Kommunikationsstart, -ende, Reintegration) - Bearbeitung von Verbindungszusammenbrüchen	
4	Transport (Transport)	- Logische Adressierung der Prozesse auf den Endgeräten - Fehlersicherungs- und Fehlerbehebungsverfahren - Stauvermeidung	TCP, UDP
3	Vermittlung (Network)	- Logische Adressierung der Endgeräte - Zielwegfindung (z.B. über Routingtabellen) - Flusskontrolle	IP, ICMP
2	Sicherungsschicht (Data Link)	- Physikalische Adressierung der Endgeräte - Gewährleistung einer zuverlässigen Übertragung - Definition der Arbitrationmethode bei Buskommunikation	Ethernet, Token Ring, FDDI
1	Bitübertragung (Physical)	- Übertragungsmedium / Leiter - Leitungscode / Bitkodierung - Serielle oder parallele Übertragung - Symmetrische oder nicht symmetrische Übertragung	

Tabelle 1: ISO/OSI-Referenzmodell – die ISO/OSI-Schichten

löschen“ unterscheidet. Felder, deren Inhalt innerhalb einer Telegrammverwendung variabel sind, zum Beispiel der zu übertragende Text, werden hier nicht erwähnt.

Jede Telegrammverwendung erhält einen im Rahmen dieser Schnittstelle eindeutigen Namen, welcher in den Sequenz- und Zustandsdiagrammen verwendet wird. Dadurch kann man jederzeit herausfinden, wie genau ein Telegramm für eine bestimmte Aufgabe aufgebaut sein muss.

8.1 ISO/OSI-Schichten unterhalb der Anwendungsebene

Die in der fachlichen Ebene erarbeiteten Anforderungen an die Schnittstelle beschreiben die Schnittstelle auf funktionaler Ebene. Eine Schnittstelle muss neben diesen funktionalen Anforderungen auch nichtfunktionale Anforderungen wie beispielsweise RAMS(S)-Anforderungen – also zum Beispiel Anforderungen an die Sicherheit – umsetzen. Außerdem muss eine Entscheidung bezüglich der tatsächlichen technischen Realisierung getroffen werden. Diese Umsetzung erfolgt auf der technischen Ebene. Für Schnittstellen hat sich das ISO/OSI-Referenzmodell [5] etabliert (Tabelle 1).

Die erarbeiteten fachlichen Abläufe bewegen sich hier auf der Ebene 7, der Anwendungsebene.

Das ISO/OSI-Modell ermöglicht es, durch die Schichtenarchitektur Verant-

wortlichkeiten und Aufgaben einer Netzwerkkommunikation klar zu trennen, Industriestandards für einzelne Schichten zu definieren, diese einzusetzen und einzelne Schichten austauschbar zu machen. Ein Lösungsansatz kann beispielsweise sein, für die Schichten 3 bis 4 das Netzwerkprotokoll TCP/IP einzusetzen und für die Schichten 1 bis 2 auf Industrial Ethernet aufzusetzen.

Um die Anforderungen an die Sicherheit umzusetzen, könnte als Zwischenschicht zwischen der Transportschicht (4) und der Darstellungsschicht (5) eine zusätzliche Sicherheitsschicht durch Modellierung spezifiziert und entwickelt werden.

In der SysML sind die Darstellungen dieser Schichten und deren Interaktion einfach mit Blockdefinitions- und internen Blockdiagrammen möglich.

LITERATUR

- [1] OMG Systems Modeling Language (OMG SysML) Specification.
Internet: http://www.omg.org/technology/documents/domain_spec_catalog.htm#OMGSysML, OMG
- [2] EN 50126:1999 - Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), VDE
- [3] Weillkiens, T.: Systems Engineering mit SysML/UML. dpunkt Verlag, 2. Auflage 2008
- [4] Friedenthal, S.: A Practical Guide to SysML – The Systems Modeling Language. Elsevier, 2008
- [5] Zimmermann, H.: OSI Reference Model - The ISO Model of Architecture for Open Systems Interconnection. 1980

Berner & Mattner Systemtechnik GmbH

Erwin-von-Kreibig-Str. 3
80807 München
Tel.: +49 (0)89 608090-0
Fax: +49 (0)89 6098182
info@berner-mattner.com
www.berner-mattner.com

Die Autoren



Dipl.-Ing. Thorsten Hiebenthal
Abteilungsleiter Transportation
Berner & Mattner Systemtechnik
Anschrift: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Thorsten.Hiebenthal@berner-mattner.com



Dipl.-Ing. Thomas Lauscher
Senior Systemingenieur
Berner & Mattner Systemtechnik
Anschrift: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Thomas.Lauscher@berner-mattner.com



Dipl.-Inf. Univ. Christian Fischer
Software-Ingenieur
Berner & Mattner Systemtechnik
Anschrift: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Christian.Fischer@berner-mattner.com

N°	OSI layer	Tasks	Protocol examples
7	Application	- Provide applications access to network	HTTP, FTP, HTTPS, SMTP, LDAP
6	Presentation	- Data conversion into standard format for transmission - Data compression - Data encryption	
5	Session	- Session management (Start/end of communication, reintegration) - Handling of disconnections	
4	Transport	- Logical addressing of processes at hosts - Error prevention and error correction process - Congestion control	TCP, UDP
3	Network	- Logical addressing of hosts - Routing (e.g. via routing tables) - Flow control	IP, ICMP
2	Data Link	- Physical addressing of hosts - Ensuring of reliable transmission - Definition of the arbitration method for bus communication	Ethernet, Token Ring, FDDI
1	Physical	- Transfer medium/line - Line code/bit coding - Serial or parallel transfer - Symmetrical or non-symmetrical transmission	

Table 1: The ISO/OSI layers of the reference model

Signalling systems almost exclusively use telegram-based data interfaces. Therefore, how to define interface telegrams leaving no room for interpretation is illustrated in the example below.

As an example, the upper part of figure 10 shows a structure of a data telegram, that is, its byte and bit structure. This is followed by a description of all telegram fields in the middle part. Finally, the "telegram usage" is defined for every telegram instance in the lower part.

In this context, the term telegram usage refers to a specific usage of a telegram as a command or a message. The telegram usage definition describes the content of all fields that represent the specific usage as a command or a message. In the example shown above, it only refers to the control byte because this differentiates between the two telegram usages, "send text" and "delete text". Fields are not mentioned here if their content is variable within the given telegram usage, the text to be sent, for example.

Each telegram usage is given a unique name within the context of the interface. The name is used in the sequence diagrams and statecharts, helping to determine exactly how a telegram should be composed for any given task at any time.

8.1 ISO/OSI layers below the application level

The interface requirements developed at the domain level describe the interface at the functional level. Besides these functional requirements, an interface also has to implement non-functional require-

ments such as RAM(S) requirements. Additionally, decisions have to be made regarding the actual technical implementation at the technical level. The ISO/OSI reference model [5] is widely used for interfaces (see table 1).

The developed application procedures reside on layer 7, the application layer.

Due to its layered architecture, the ISO/OSI model facilitates a clear separation of network communications responsibilities and tasks. Moreover, it helps to define and apply industry standards for individual layers and to make individual

layers replaceable. One approach could be, for example, to apply the network protocol TCP/IP for layers 3-4 and to use Industrial Ethernet for layers 1-2.

To meet safety requirements, an intermediate safety layer between the transportation layer (4) and the presentation layer (6) could be specified and developed by modelling.

SysML facilitates the presentation of these layers and their interactions with block definition diagrams and internal block diagrams.

LITERATURE

- [1] OMG Systems Modeling Language (OMG SysML) Specification, Internet: http://www.omg.org/technology/documents/domain_spec_catalog.htm#OMGSysML, OMG
- [2] EN 50126:1999 – Spezifikation und Nachweis der Zuverlässigkeit, Verfügbarkeit, Instandhaltbarkeit und Sicherheit (RAMS), VDE
- [3] Weilkiens, T.: Systems Engineering mit SysML/UML, dpunkt Verlag, 2. Auflage 2008
- [4] Friedenthal, S.: A Practical Guide to SysML – The Systems Modelling Language, Elsevier, 2008
- [5] Zimmermann, H.: OSI Reference Model-The ISO Model of Architecture for Open Systems Interconnection, 1980

Berner & Mattner Systemtechnik GmbH

Erwin-von-Kreibig-Str. 3
80807 München
Tel.: +49 (0)89 608090-0
Fax: +49 (0)89 6098182
info@berner-mattner.com
www.berner-mattner.com

The authors



Dipl.-Ing. Thorsten Hiebenthal
Head of Transportation
Berner & Mattner Systemtechnik
Address: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Thorsten.Hiebenthal@berner-mattner.com



Dipl.-Ing. Thomas Lauscher
Senior Systems Engineer
Berner & Mattner Systemtechnik
Address: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Thomas.Lauscher@berner-mattner.com



Dipl.-Inf. Univ. Christian Fischer
Software Engineer
Berner & Mattner Systemtechnik
Address: Erwin-von-Kreibig-Straße 3, D-80807 München
E-Mail: Christian.Fischer@berner-mattner.com