Pflichtenheft

Für das studentische Projekt „Sichere Eisenbahnsteuerung“

Beschreibung:	**Klärung der Anforderungen an das System, welche von Prof. Dr. J. Bredereke gestellt werden**
Autor/en:	Ole Bohn Felix Geber
Ablageort:	Dokumente\01_Anforderungsanalyse\01.00_Pflichtenheft \01.00.02_noch nicht freigegebene Dokumente\Pflichtenheft.pdf
Version:	0.20
Status:	In Bearbeitung
Datei:	Pflichtenheft.pdf
Datum:	08.04.2010

1 Änderungshistorie

Version	Datum	Autor/en	Änderungsgegenstand
0.00	31.03.10	Ole Bohn, Felix Geber	Anpassung des Pflichtenhefts aus dem WiSe09/10 an die Anforderungen des SoSe10
0.10	03.04.10	Ole Bohn	Anpassen aller Kapitel an die Veränderungs-vorschläge von Herrn Bredereke in der Mail vom 01.04.10
0.11	07.04.10	Felix Geber	Layout-Anpassung
0.20	08.04.10	Ole Bohn, Felix Geber	Anpassung der Systemgrenzen (4.2), Ergänzung der Testziele im Kapitel 7 „Funktionsprüfung“
0.21	08.04.10	Ole Bohn, Felix Geber	Anpassung der Änderungshistorie

2 Inhaltsverzeichnis

3 Begriffe und Abkürzungen

In diesem Abschnitt werden die für dieses Projekt relevanten, jedoch nicht allgemein gebräuchlichen Begriffe und Abkürzungen kurz dargestellt.

3.1 Begriffe

Rangierbetrieb: Die Lok fährt mit langsamer Geschwindigkeit und bewegt Wagons zum Rangieren.

Zugbetrieb: Die Lok fährt mit möglichst konstanter und hoher Geschwindigkeit mit oder ohne Wagons. Im Zugbetrieb darf sich nur eine Lok in einem Gleisabschnitt befinden.

Fahraufgabe: Die Fahraufgabe beschreibt das Verhalten einer Lok im Rangier- und Zugbetrieb. Sie definiert das Schema, nach dem die beiden Loks sich auf der Strecke bewegen.

XpressNet: Ein von Lenz Elektronik entwickeltes Netzwerk zur Verbindung von Eingabegeräten zur Steuerung einer Modelleisenbahn. Typischerweise werden DCC-Bauteile (Loks, Weichen, etc.) hierüber angesteuert. Nähere Information zum XpressNet Netzwerk befinden sich in der Aulis Gruppe.

S88: Ein System, das Sensoren Rückmeldung von Ereignissen ermöglicht (z. B. das Überfahren eines Gleisabschnitts). Nähere Information zum S88 Bus befinden sich in der Aulis Gruppe. Nähere Informationen sind in der Aulis Gruppe zu finden.

Railcom: Ein erweitertes Rückmeldesystem

Notfallsignal: Das Notfallsignal lässt alle Loks auf der Strecke sofort stehen.

DCC: Über DCC werden die Lokomotiven, Weichen und Signale (wie z.B. Licht) über die Schienen der Modelleisenbahn digital gesteuert. Nähere Informationen sind in der Aulis Gruppe zu finden.

SSC: SSC ist eine Schnittstelle zur synchronen, seriellen Datenübertragung. Signale sind nur dann gültig, wenn ein beidseitig genutzter Takt einen bestimmten, vordefinierten Zustand annimmt (z.B. eine positive Flanke). Nähere Informationen sind in der Aulis Gruppe zu finden.

3.2 Abkürzungen

DCC – Digital Command Control

SSC – Synchronous Serial Channel

FTA – Failure Tree Analysis

FMEA – Failure Mode and Effects Analysis

4 Zielsetzung

4.1 Allgemeine Beschreibung

Das vorliegende Dokument stellt das Pflichtenheft zum Projekt „Sichere Eisenbahnsteuerung“ im Sommersemester 2010 dar. Dieses Projekt schließt an begonnene Aktivitäten aus dem Wintersemester 2009/2010 an.

Ziel dieses Projekts ist es, den Funktionsumfang aus dem Vorgängerprojekt vollständig zu erfüllen und ggf. um einige, noch festzulegende Details, zu erweitern.

Primäre Problemstellung ist es, die Lauffähigkeit der im Wintersemester erarbeiteten Anlage herzustellen. Erst wenn dies erfolgt ist, kann die Funktionalität um weitere Details ergänzt werden.

4.2 System-Umgebung

Das Projekt „Sichere Eisenbahnsteuerung“ befasst sich mit der Entwicklung einer Eisenbahnsteuerung, welche sicherstellt, dass es zu keinem Zeitpunkt zu einem unsicheren Zustand auf den Gleisanlagen kommen kann.

Das zu entwickelnde System besitzt die in Abbildung 1 dargestellten Grenzen. Somit gehören sowohl die Gleisanlagen, die Stromversorgung, der Benutzer und der Anwender zur Systemumgebung. Dem Benutzer werden über eine noch festzulegende Form der Visualisierung mögliche Operationen angeboten und er kann über Tastendrücke Aktionen ausführen.

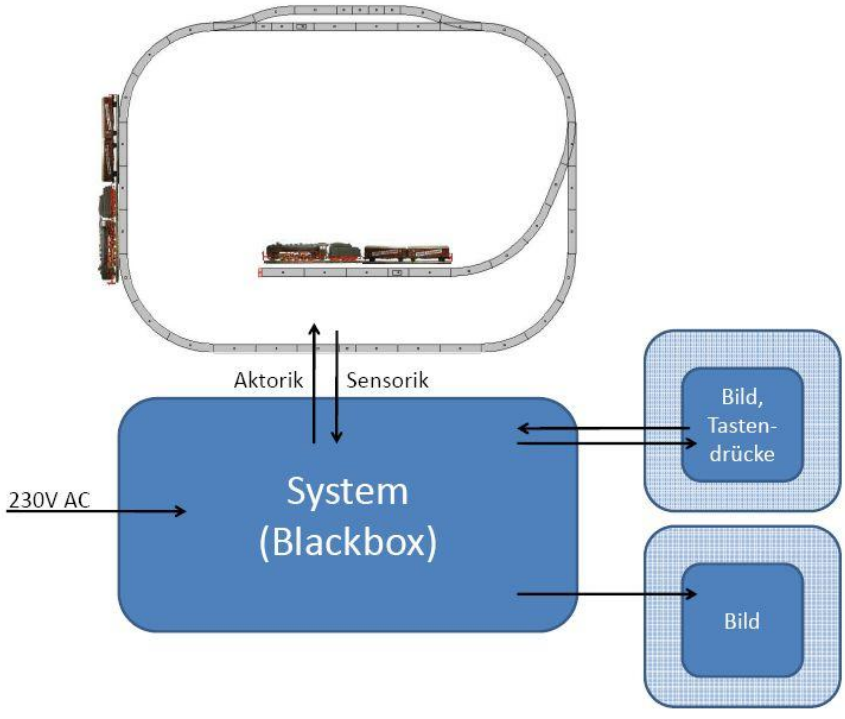

Abb. 1: Schematische Darstellung der Systemgrenzen

4.3 Projektstruktur

Wie bereits kurz in der allgemeinen Beschreibung angedeutet, handelt sich bei dem Projekt „Sichere Eisenbahnsteuerung“ im Sommersemester 2010 um eine Fortführung eines Projekts aus dem Wintersemester 2009/2010.

Im Wintersemester ist das Projektteam mit der nachfolgend beschriebenen Aufgabenstellung gestartet. Die komplette von Herrn Prof. Dr. Bredereke verfasste Aufgabenstellung kann in der Aulis Gruppe des Wintersemester Projekts nachgelesen werden. Der Pfad dazu lautet*: Aulis → F4 TI PROJEKT Bredereke → WiSe0910 → Beamerfolien Bredereke → 01c_Aufgabenbeschreibung.*

Die Studierenden erhielten die Aufgabe, ein sicherheitsrelevantes eingebettetes System zu entwickeln. Bei dem System handelt es sich um die bekannte Eisenbahnsteuerung am Beispiel einer Modelleisenbahn. Die Eisenbahnsteuerung sollte hierbei sicherstellen, dass das System eine vorgegebene Rangieraufgabe löst, ohne dass es zu unsicheren Zuständen auf der Anlage kommt.

Der Entwicklungsprozess sollte nach dem allgemein bekannten V – Modell aus ProVISTA erfolgen. Die zu entwickelnde Software sollte in der Programmiersprache C geschrieben werden und auf einem Mikrokontroller des Typs C515C laufen. Wichtig hierbei ist, dass der Entwurf der Software nach den Kriterien sicherheitsrelevanter Systeme erfolgt. Jeder Entwicklungsschritt ist durch geeignete Tests abzusichern.

Das System sollte schließlich an den XpressNet Bus einer Modellbahnsteuerung angeschlossen werden. Zusätzlich dazu ist ein geeignetes Rückmeldesystem über den Zustand der Gleise zu installieren und mit dem XpressNet Bus zu verbinden. Die nötigen Kenntnisse zu den einzelnen eingesetzten Technologien sind eigenständig in Vorträgen oder ähnlichem zu erarbeiten.

Zusätzlich zu den theoretischen Entwurfsaufgaben erhielten die Studierenden die Aufgabe, eine Modelleisenbahnanlage im Rahmen des Projekts zu beschaffen und aufzubauen.

Am Ende des Semesters wurde folgender Zustand erreicht: Ein erster Entwurf der Software wurde in der Programmiersprache C fertiggestellt und in einem ersten Schritt einfachen Tests unterzogen. Es ist jedoch festzuhalten, dass die Software sowohl im Simulator, als auch auf der Eisenbahnanlage nicht lauffähig ist.

Die Hardware der Anlage hingegen ist vollständig funktionsfähig und im Projektraum aufgebaut. Realisiert wurde die Steuerung mit zwei redundanten Mikrokontrollern vom Typ C515C. Zur Verbindung der einzelnen Teilnehmer wurde das XpressNet Netzwerk genutzt, als Rückmeldesystem für den Zustand der Gleise wurde S88 eingesetzt.

Im folgenden Abschnitt wird nun die Aufgabenbeschreibung des Folgeprojekts im Sommersemester 2010 beschrieben. Dieses baut auf die Ergebnisse des im vorangegangen Semesters ausgeführten Projekts auf.

Die Aufgabenbeschreibung für das Folgeprojekt stammt ebenfalls von Herrn Prof. Dr. Bredereke und ist in vollständiger Länge in der Aulis Gruppe des Sommersemesterprojekts nachzulesen (Pfad: *Aulis → F4 TI PROJEKT Bredereke WiSe0910 → Beamerfolien Bredereke → 01c_Aufgabenbeschreibung*).

Hauptaugenmerk liegt in diesem Semester auf der Fertigstellung der Software aus dem Wintersemester. Die Entwicklung der ersten Version ist abzuschließen und ausführlichen Test zu unterziehen. Darüber hinaus sollen weitere Funktionalitäten ergänzt werden.

Die Weiterentwicklung bzw. Neuentwicklung soll sich wiederum an dem Vorgehensmodell nach ProVISTA orientieren, dabei im speziellem am V – Modell.

Die möglichen Teilaufgaben dieses Semesters sind nachfolgend aufgelistet. Je nach zeitlichem Spielraum werden die einzelnen Punkte abgearbeitet.

Ergänzende Funktionalität:

- ein Algorithmus, um die Startposition des rollenden Materials automatisch zu ermitteln (Dazu müssen die Loks langsam losfahren, bis sie Sensoren überfahren, und die Anhänger müssen sozusagen „im Dunklen“ vorsichtig gesucht werden.)
- als ersten Schritt dahin die Fähigkeit zum Neustart, ohne die Software neu in die Mikrocontroller laden zu müssen _ ein Algorithmus zum Vergleich der Ergebnisse der beiden redundanten Mikrocontroller, der mit mehr Arten von unbedeutenden Abweichungen zurechtkommt
- ein Algorithmus für die Fahrstraßenplanung, der durch hinreichende Vorausschau ein gegenseitiges Blockieren der einzelnen Fahrprogramme verhindert
- ein Algorithmus für die Fahrstraßenplanung, der niemals auch nur kurzzeitig einen kritischen Zustand zulässt, und dazu eine Anpassung der Befehlsvalidierung, die dann bei jedem kritischen Zustand nunmehr sofort ein Not-Aus auslöst
- Auswertung des Sicherheits-Audits.

Ergänzende Sicherheitsthemen:

- ein automatischer vollständiger Regressionstest der Software
- ein Nachweis, dass die Kriterien der Befehlsvalidierung hinreichend sind
- eine Fehlerbaumanalyse, um systematische Fehler im Entwurf zu finden (mind. ein Fehler ist dem Veranstalter schon bekannt)
- ein Zeit-Budget aufstellen und nachweisen, dass es stets eingehalten wird (dies ist nach Meinung des Veranstalters zur Zeit nicht der Fall)
- Trennung der äußeren Schnittstellen und der inneren Struktur in den Entwurfsdokumenten (verbessert die Verständlichkeit und Wartbarkeit des Systems; diese Tätigkeit kann zur Einarbeitung für neue Teilnehmer dienen)
- ausgewählte Algorithmen mittels eines Model-Checkers für C-Code verifizieren (d.h. automatisch vollständig testen)

5 Voraussetzungen

5.1 Hardware-Umgebung

Für die Realisierung der definierten Fahraufgaben (siehe Abschnitt 6.1.1/6.1.2) ist der Aufbau einer digitalen, DCC-fähigen Modelleisenbahn der Spur H0 vorzunehmen.

Die Strecke soll aus einem ovalen Ring, einem Abstellgleis und einem Nebengleis bestehen. Die Gleisabschnitte müssen dabei lang genug sein, sodass alle Wagons, sowie die Lokomotiven gemäß der gewählten Fahraufgabe unterzubringen sind. Die Steuerung der DCC-Lokomotiven soll über eine XpressNet-Verbindung durch zwei Mikrocontroller vorgenommen werden.

Zur Verfügung stehen hier die C515C-Mikrocontroller im Labor für Computertechnik (hierdurch ergeben sich implizite Anforderungen, z. B. durch die vorhandene Taktfrequenz und Speicherkapazität). Sie verfügen über eine RS232-Schnittstelle, die über einen Adapter an den RS-485-Bus des XpressNet Netzwerks angeschlossen werden kann.

Rückmeldungen über die Zustände des Eisenbahnsystems werden durch Hall Sensoren vorgenommen. Die Signale werden über eine geeignete Schnittstelle zum Mikrocontroller per S88 gesendet.

5.2 Software-Umgebung

Zur Softwareumgebung zählt die ausschließlich die Ablaufumgebung für die Software auf dem PC sowie die Bibliothek des I²C – Busses. Auf dem Mikrokontroller existiert kein Betriebssystem.

Als Ablaufumgebung wurde Keil µVision4 gewählt. Die Programmierung der Software erfolgt in der Programmiersprache C.

5.3 Entwicklungshilfsmittel

Im Rahmen dieses Projekts werden folgende Entwicklungshilfsmittel verwendet: Keil µVision4, Google – Code sowie Aulis.

Bei Keil µVision4 handelt es sich um eine Entwicklungsumgebung zur Programmierung von Mikrokontrollern. Die Programmierung erfolgt hierbei in der Programmiersprache C. Keil µVision4 stellt weitgehende Möglichkeiten zur Verfügung, auch zum Testen bzw. Debuggen der entwickelten Software.

Bei Google – Code handelt es sich um ein Versionsverwaltungssystem, mit dessen Hilfe der erzeugte Programmcode immer auf einem aktuellen Stand gehalten wird und für alle Projektmitglieder zugänglich bleibt. Neben der Verwaltung des Programmcodes werden mittels Google – Code auch alle relevanten Entwicklungsdokumente verwaltet. Dies bietet die analogen Vorteile wie beim Programmcode.

Das System Aulis stellt die online – Lernplattform der Hochschule Bremen dar. Hierauf können Ordnerstrukturen erzeugt werden, in denen Daten abgelegt werden können. Auch hierauf haben alle Projektmitglieder Zugriff.

5.4 Randbedingungen

Wie bereits in vorangegangenen Abschnitten beschrieben, handelt es sich beim vorliegenden System um ein sicherheitsrelevantes. Aus diesem Grund ist es wichtig, dass die Entwicklung des Systems den Vorschriften zur Entwicklung sicherheitsrelevanter Systeme gehorcht.

Für ein sicherheitsrelevantes System ist es wichtig, dass es zu keinem Zeitpunkt zu einem unsicheren Zustand kommt. Auch darf ein Ausfall von Hardware nicht zu einem unsicheren Zustand führen. Das heißt sowohl Software- als auch Hardware müssen so ausgelegt sein, das beim Ausfall einzelner Komponenten ein sicherer Ablauf gewährleistet ist.

Nähere Informationen zum Entwurf sicherheitsrelevanter Systeme können in der Aulis Gruppe des Wintersemester Projekts nachgelesen werden.

6 Funktionsumfang

Das System soll eine vordefinierte Fahraufgabe lösen. Oberstes Ziel ist es, dass es zu keinem Zeitpunkt zu einem unsicheren Zustand des Systems kommt (Kollision auf dem Gleis etc.).

Ein Schwerpunkt liegt bei der automatischen Steuerung des Systems, die einen kollisionsfreien Zugverkehr anstreben soll. Ein anderer ist die Gewährleistung der Systemsicherheit zu jedem Zeitpunkt. Hierfür startet das System in einem vordefinierten, sicheren Zustand.

Des Weiteren soll das Auslesen der Informationen eines Sicherheits-Audits in Klartext erfolgen.

6.1 Aufgaben / funktionale Anforderungen

Die Lokomotiven fahren vorwärts gegen den Uhrzeigersinn auf der Kreisbahn. Die Rangierlokomotive kann auch rückwärts (d. h. mit dem Uhrzeigersinn) fahren. Lok #1 fährt immer im Zugbetrieb, d.h. mit hoher Geschwindigkeit (konstant, falls sie nicht vom Rangierbetrieb gestört wird). Lok #2 ist immer für den Rangierbetrieb zuständig und startet vom Abstellgleis. Es gibt eine erste Fahraufgabe sowie eine optionale zweite, die sich nur im Rangierbetrieb von der ersten unterscheidet. (Entnommen: Fahraufgaben, siehe Literaturverzeichnis)

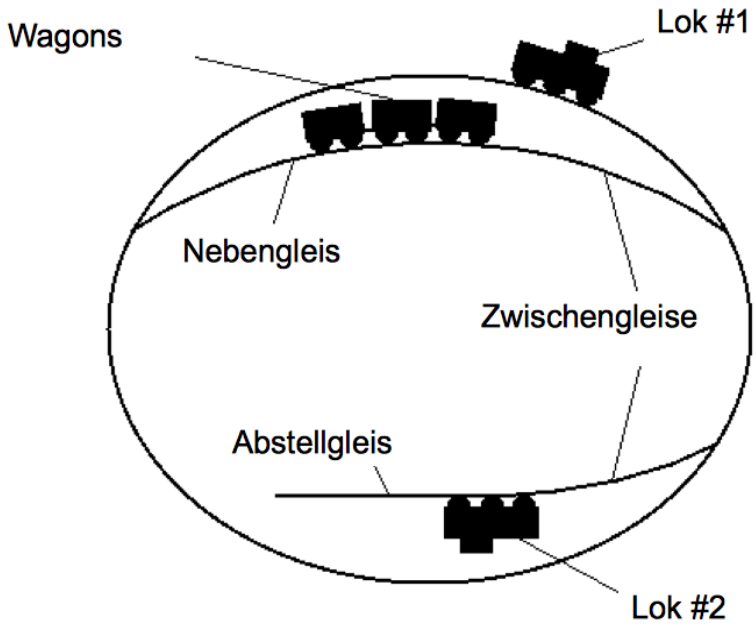

Abbildung 1: Darstellung der Fahraufgabe

6.1.1 Erste Fahraufgabe

Lok #2 hat die Aufgabe alle Wagons (auf einmal) vom Nebengleis auf das Abstellgleis zu bringen, dabei schiebt sie die Wagen im Uhrzeigersinn dorthin. Dann koppelt sie die Wagen ab und fährt selbst zurück zum Nebengleis, um dort zu warten. Anschließend geht das ganze andersherum: Die Lok fährt vom Nebengleis zum Abstellgleis, koppelt die Wagen an, zieht sie gegen den Uhrzeigersinn auf das Nebengleis, koppelt sie ab und fährt auf das Abstellgleis. Die Lok #2 wartet also immer dort, wo die Wagons gerade nicht sind, für eine variable Zeit.

6.1.2 Zweite Fahraufgabe (optional)

Lok #2 sortiert (mindestens) drei Wagons um, die auf dem Nebengleis stehen. Wenn man im Ausgangszustand die Wagen von links nach rechts mit eins bis drei durchnummeriert, sollen sie am Ende der Aufgabe in der Reihenfolge 3,2,1 stehen. Für die Sortierung wird das Abstellgleis benutzt. Die Lokomotive koppelt den ersten Wagen von links an, zieht ihn auf das Abstellgleis und koppelt ihn dort ab. Dieser Vorgang wird so lange wiederholt, bis alle Wagen auf dem Abstellgleis stehen. Dann nimmt sie alle auf einmal und bringt sie auf das Nebengleis. Dort wartet die Lok für eine variable Zeit und sortiert wieder von vorne.

6.2 Benutzungsschnittstellen und -einrichtungen

Die Kommunikation zwischen System und Systemumgebung erfolgt über die Schnittstellen RS–232, XpressNet und S88.

Sowohl die Multimaus, als auch der PC (über das Interface LI101F) sind mittels XpressNet mit der DCC Command Station verbunden. Diese gibt schließlich die Signale zur Steuerung an die Gleisanlagen und Weichen weiter.

Die Kommunikation der Mikrokontroller mit der DCC Command Station erfolgt ebenfalls über XpressNet. Allerdings ist hierbei zu berücksichtigen, dass die Mikrokontroller nur eine RS–232-Buchse besitzen. Aus diesem Grund muss die Verbindung zum XpressNet über einen Adapter hergestellt werden.

Die Kommunikation mit den Hall Sensoren, welche Signale über Zustand der Züge auf den Gleisen erhalten, mit dem System erfolgt über die S 88 Schnittstelle.

Nähere Informationen zur Funktionsweise der einzelnen Schnittstellen können in der Aulis Gruppe des Sommersemester Projekts nachgelesen werden.

6.3 Quantitative Anforderungen

Das System muss jederzeit so schnell reagieren, dass auf keinem Gleisabschnitt unsichere Zustände auftreten können. Detailliertere Angaben zu den hier nötigen Anforderungen sind im weiteren Verlauf des Projekts vom Projektteam zu erarbeiten.

6.4 Konfigurationen, Ausbaustufen, Varianten

Es sind keine weiteren Ausbaustufen oder Varianten der Anlage vorgesehen. Der Entwurf muss dies nicht berücksichtigen.

6.5 Kompatibilität, Portabilität

Das System stellt eine Neuentwicklung dar, welche im Rahmen des Projekts im Wintersemester 2009/2010 erstellt wurde. Bzgl. der Kompatibilität werden keine gesonderten Anforderungen gestellt, ausgenommen, dass alle neu hinzugefügten Funktionalitäten im Sommersemester 2010 mit den Vorleistungen aus dem Wintersemester kompatibel sein müssen.

Ein vollständiger Neuentwurf des Systems ist nicht anzustreben, vielmehr sollen nur Erweiterungen vorgenommen werden.

An die Portabilität des Systems werden ebenfalls keine besonderen Anforderungen gestellt. Es ist nicht erforderlich, dass das System in einer anderen Systemumgebung, das heißt z.B. auf einer anderen Gleisanlage, ebenfalls funktionsfähig ist. Der Entwurf ist explizit auf die vorhandene Infrastruktur und deren Anforderungen angepasst worden.

7 Funktionsprüfung

7.1 Anwendung(-sschicht)

- Fährt die Bahn in die richtige Richtung?
- Wird die Fahraufgabe korrekt umgesetzt?
- Werden Kollisionen vermieden?
- Wird das Verlieren von Wagons ermittelt?
    - Voraussetzung: Gesamtanzahl und Startposition der Wagons bekannt
- Reagiert die Software angemessen auf Signale der Hardware?
- Funktioniert die Gleisfreiheitsprüfung?

7.2 Sicherheit(-sschicht)

- Reagiert die Software angemessen auf Signale der Hardware?
- Stimmt die Anzahl der Wagons hinter dem Triebwagon nach Koppelvorgang?
- Funktioniert die Gleisfreiheitsprüfung?
- Werden Kollisionen verhindert?

7.3 Hardware(-komponenten)

- Sind die Weichen verstellbar?
- Liefern die Sensoren korrekte Daten?

7.4 Schnittstellen

- Werden die Anweisungen der Anwendung in korrekte DCC-Befehle umgesetzt?
- Werden die Hardware-Signale von der Software korrekt ausgewertet?

8 Literaturverzeichnis

- Aulis → F4 TI PROJEKT Bredereke → WiSe0910 → Beamerfolien Bredereke → 01c_Aufgabenbeschreibung
- ProVISTA → Methoden → Anforderungsanalyse → Pflichtenheft