Formale Spezifikation in Reverse-Engineering-Prozessen für technische Systeme

von

Jörg Lange

Motivation

- Verbesserung der Dokumentation des XCTL-Systems
- Fehler, Ungenauigkeiten finden
- Erstellen von formalen Spezifikationen in der Z-Notation
- kritische Betrachtung der verbalen Spezifikation

Reverse-Engineering

- Prozess zur Analyse eines bestehenden Systems
- Beschreibung von Systemkomponenten
- Erstellung oder Vervollständigung von Dokumenten

Formale Methoden

- präzise und eindeutige Beschreibungstechnik
- Vorteil gegenüber natürlicher Sprache
- Möglichkeit der Qualitätsverbesserung von Software
- höherer Aufwand

Z-Notation

- erdacht Ende der 70er Jahre von Abrial
- weiterentwickelt von „Programming Research Group“ der Universität Oxford
- 2002 durch ISO standardisiert
- soll vom Menschen gelesen werden

Z-Notation

- basiert auf Mengenlehre und Prädikatenlogik
- Strukturmittel: Schema
- strenges Typkonzept
- Typen sind Mengen

Beispiel: Z-Notation - Geburtstagsbuch

[NAME, GEBURTSDATUM] ← Basistypen

Geburtstagsbuch

$personen : \mathbb{P}\ NAME$

$geburtstag : NAME \pfun GEBURTSDATUM$ ← Schema

$personen = \mathbf{dom}\ geburtstag$

personen = {John, Mike, Susan}
geburtstag = {John ↦ 25-Mar, Mike ↦ 20-Dec, Susan ↦ 20-Dec}

Beispiel: Z-Notation - Geburtstagsbuch

- Operation: Geburtstag hinzufügen

Geburtstag_hinzufügen

Δ Geburtstagsbuch
name? : NAME
datum? : GEBURTSDATUM

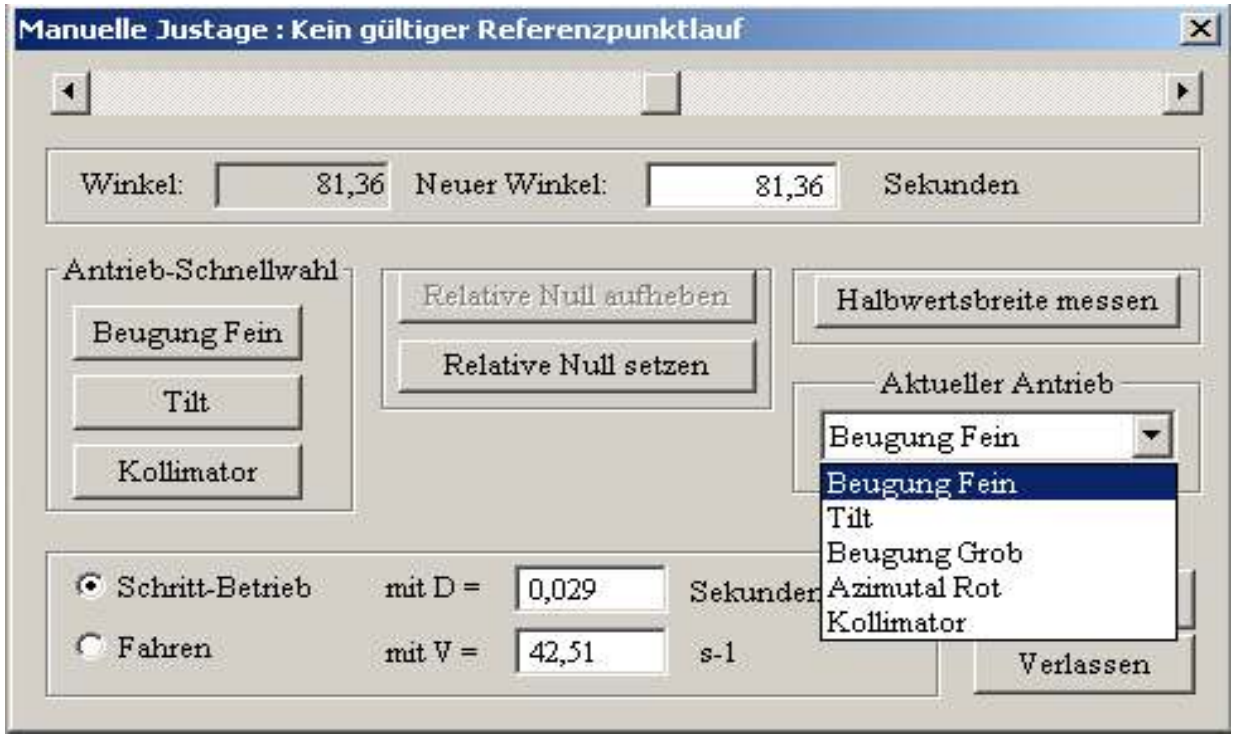
---

name? $\notin$ personen
geburtstag' = geburtstag $\cup$ { name? $\mapsto$ datum?}

Ziele der Arbeit

- formale Spezifikation von „Manuelle Justage (alt)“
- formale Spezifikation von „0-dim. Detektoren, Zählerfenster“
- Einbeziehung des Zeitaspektes
- Hervorhebung erkannter Probleme in verbalen Spezifikationen

Manuelle Justage (Alt)



- Teilfunktion von XCTL
- Steuerung von fünf Antrieben / Motoren

Manuelle Justage (Alt)

- Ausgangspunkt: Pflichtenheft und XCTL-Programm
- verwendete Typen
- Identifikation eines Systemzustands
- Identifikation von Operationen

Manuelle Justage (Alt) – verwendete Typen

EREIGNISSE ::= *Links*
| *Enter*
| *Rechts*
| *Ausfuehren_Manuelle_Justage_Alt*
| *Verlassen_Manuelle_Justage*
| *Verlassen_XCTL*
| *Setze_Relative_Null*
| *Relative_Null_Aufheben*

ANTRIEBSART ::= *fahrbetrieb* | *schrittbetrieb*

ANTRIEB ::= *DC* | *DF* | *AR* | *TL* | *CC*

STATUS ::= *Ein* | *Aus*

Manuelle Justage (Alt) - Systemzustand

- Position der fünf Antriebe
- relative Null – gesetzt / nicht gesetzt
- .ini – Dateien
- aktuelle Geschwindigkeit, aktuelle Schrittweite
- aktuell gewählter Antrieb
- aktuelle Antriebsart

Manuelle Justage (Alt) – Systemzustand

INI_File

$$dc\_ist\_position, dc\_position\_min, dc\_position\_max, dc\_schrittweite, dc\_schrittweite\_min, dc\_schrittweite\_max, dc\_geschwindigkeit, dc\_geschwindigkeit\_max : \mathbb{Z}$$

Manuelle Justage (Alt) – Systemzustand

XCTL

$$
\begin{array}{|l}
\hline
INI\_File \\
dc\_rel\_null,\ dc\_rel\_ist\_position, \\
dc\_rel\_position\_min,\ dc\_rel\_position\_max : \mathbb{Z} \\
aktueller\_antrieb : ANTRIEB \\
manuelle\_justage : STATUS \\
\hline
dc\_rel\_position\_min = dc\_position\_min - dc\_rel\_null \\
dc\_rel\_position\_max = dc\_position\_max - dc\_rel\_null \\
\hline
\end{array}
$$

Manuelle Justage (Alt) – Systemzustand

Manuelle_Justage

$$
\begin{array}{l}
XCTL \\
dc\_schrittweite\_aktuell,\ dc\_geschwindigkeit\_aktuell, \\
dc\_geschwindigkeit\_aktuell\_2 : \mathbb{Z} \\
aktuelle\_antriebsart\_dc : ANTRIEBSART
\end{array}
$$

Manuelle Justage (Alt) – Operationen

- Bewegung der Antriebe (Direktbetrieb, Schrittbetrieb, Fahrbetrieb)
- Wechsel der Antriebe
- Wechsel der Antriebsart
- Setzen / Aufheben der relativen Null
- Änderung der Schrittweite und der Geschwindigkeit
- Beenden von Manuelle Justage (Alt) und von XCTL

Manuelle Justage (Alt) – Operationen

Beispiel: Direktbetrieb des Antriebs DC

Direktbetrieb_DC

Δ *Manuelle_Justage*
neuer_winkel?: $\mathbb{Z}$
eingabe?: *EREIGNISSE*

---

manuelle_justage = *Ein*
aktueller_antrieb = *DC*
eingabe? = *Enter*
if *neuer_winkel?* < *dc_rel_position_min*
then *dc_rel_ist_position'* = *dc_rel_position_min*
else if *neuer_winkel?* > *dc_rel_position_max*
then *dc_rel_ist_position'* = *dc_rel_position_max*
else *dc_rel_ist_position'* = *neuer_winkel?*

ΔManuelle_Justage $\widehat{=}$ Manuelle_Justage $\wedge$ Manuelle_Justage'
Deklaration der Variablen:
neuer_winkel? für die Eingabe der Sollposition
eingabe? für die Eingabe Enter

Bedingungen für die Nutzereingabe und den Status von Manuelle Justage (Alt)

In Abhängigkeit der Eingabe (neuer_winkel?) gilt im Folgezustand eine neue relative Ist-Position (dc_rel_ist_position').

Manuelle Justage (Alt) – Operationen

Beispiel: Auswahl eines Antriebs

Auswahl_Antrieb

$\Delta XCTL$
neuer_antrieb?: ANTRIEB

---

manuelle_justage = Ein
aktueller_antrieb' = neuer_antrieb?

Manuelle Justage (Alt) – Operationen

Beispiel: Manuelle Justage verlassen

Manuelle_Justage_Verlassen

$\Delta XCTL$
eingabe?: EREIGNISSE
dc_antrieb_ist_position?, df_antrieb_ist_position?,
tl_antrieb_ist_position?, ar_antrieb_ist_position?,
cc_antrieb_ist_position?: Z

---

eingabe? = Verlassen_Manuelle_Justage
dc_rel_ist_position' = dc_antrieb_ist_position? - dc_rel_null

Manuelle Justage (Alt) – Zeitaspekt

Beispiel: Operation – Bewegung im Fahrbetrieb

- Dauer der Eingabe bestimmt neue Position
- Zeitmodell von Coombes und McDermid → Intervallmodell
- Beschreibung mit Intervallen
- Dauer eines Intervalls kann bestimmt werden

Formale Spezifikation in Reverse-Engineering-Prozessen für technische Systeme

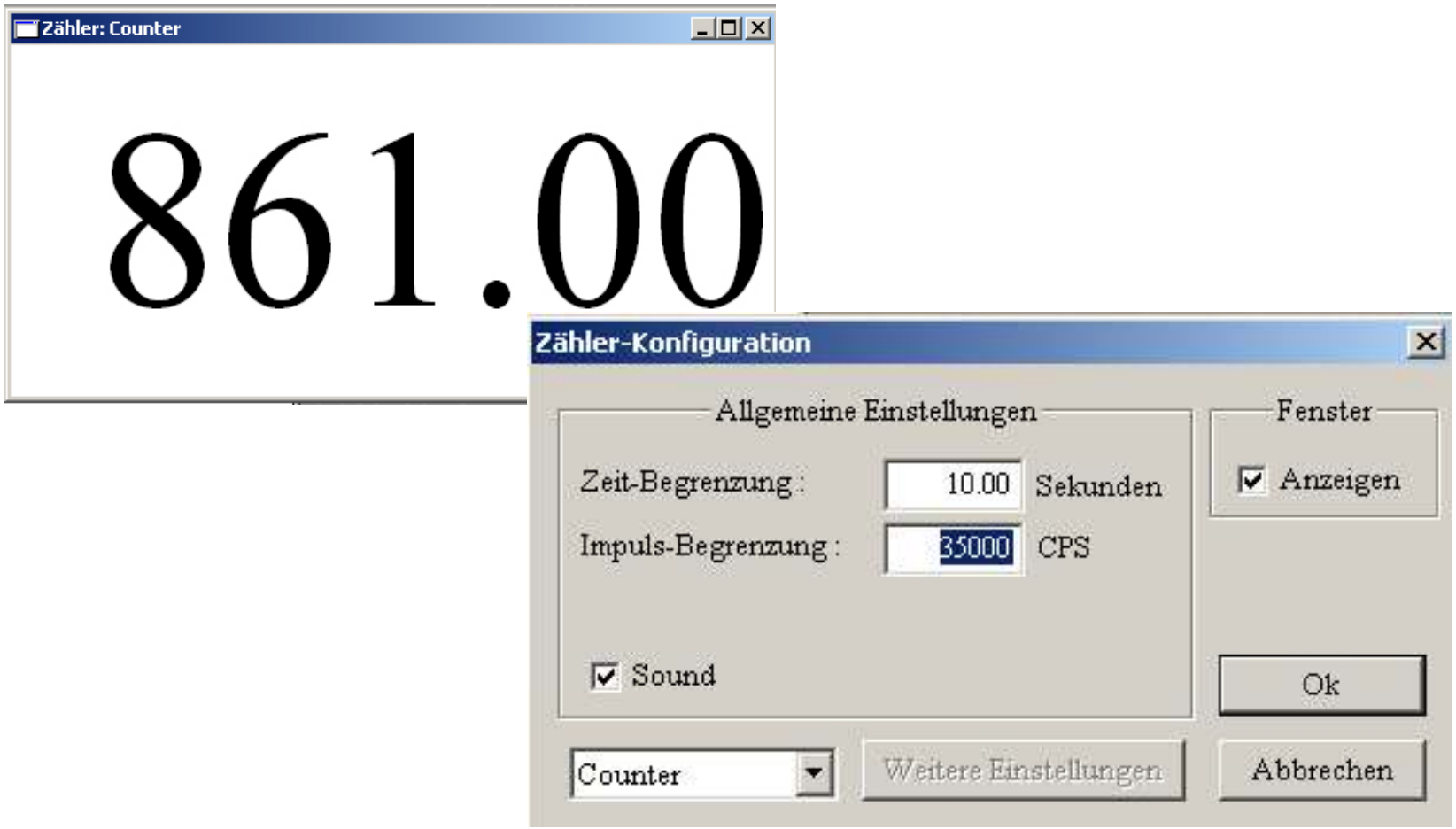
Fahrbetrieb_DC

Δ*Manuelle_Justage*
eingabe?: EREIGNISSE
laenge_der_eingabe: INTERVAL

---

manuelle_justage = Ein
aktueller_antrieb = DC
aktuelle_antriebsart_dc = fahrbetrieb
if *eingabe? = Links* $\wedge$ *dc_geschwindigkeit_aktuell > 0*
$\wedge$ *dc_rel_ist_position - dc_geschwindigkeit_aktuell * period laenge_der_eingabe*
< dc_rel_position_min
then *dc_rel_ist_position' = dc_rel_position_min*
else *dc_rel_ist_position'*
*= dc_rel_ist_position − dc_geschwindigkeit_aktuell * period laenge_der_eingabe*
$\vee$ (**if** *eingabe? = Rechts* $\wedge$ *dc_geschwindigkeit_aktuell > 0*
$\wedge$ *dc_rel_ist_position + dc_geschwindigkeit_aktuell * period laenge_der_eingab*
> dc_rel_position_max
then *dc_rel_ist_position' = dc_rel_position_max*
else *dc_rel_ist_position' = dc_rel_ist_position*
*+ dc_geschwindigkeit_aktuell * period laenge_der_eingabe*)
$\vee$ *dc_geschwindigkeit_aktuell = 0*
$\wedge$ *eingabe? = Links*
$\wedge$ *dc_rel_ist_position' = dc_rel_position_min*
$\vee$ *dc_geschwindigkeit_aktuell = 0*
$\wedge$ *eingabe? = Rechts*
$\wedge$ *dc_rel_ist_position' = dc_rel_position_max*

0-dim. Detektoren, Teilfunktion Zählerfenster



0-dim. Detektoren, Teilfunktion Zählerfenster

- Ausgangspunkt: Pflichtenheft und XCTL-Programm
- verwendete Typen
- Identifikation eines Systemzustands
- Identifikation von Operationen

Zählerfenster – verwendete Typen

DETEKTOR ::= detektor ⟪ℕ⟫

DETEKTORTYP ::= RADICON | GENERIC | BRAUN_PSD | Test | Simulant | PSD

STATUS ::= Ein | Aus

XCONTROLSTARTUP ::= Startup_Nothing

| *Startup*

| *Startup_Scan*

| *Startup_AreaScan*

| *Startup_Device*

| *Startup_ManualAdjustment*

| *NIL*

ANZEIGE ::= Digital | Balken

Zählerfenster – verwendete Typen

EREIGNISSE ::= Verlassen_Zaehler_Konfiguration
| *Verlassen_XCTL*
| *Verlassen_Zaehler_Fenster*
| *Abbrechen*
| *OK*
| *Markierung_Sound*
| *Markierung_Digitale_Anzeige*
| *Markierung_Balken_Darstellung*
| *Markierung_Fenster*
| *Markierung_Logarithmische_Dartsellung*
| *Markierung_Log_Datei*
| *Auswahl_Detektoren_Detektoren*
| *Auswahl_Einstellungen_Geraet*
| *Auswahl_Einstellungen_Anzeige*
| *Auswahl_Detektor*
| *Schließen*
| *Enter*

Zählerfenster – Systemzustand

INI_File

$Detektoren: \mathbb{P}\ DETEKTOR$
$Zeitbegrenzungen\_Default: \mathbb{P}\ (DETEKTOR \times HUNDERTSTEL)$
$Impulsbegrenzungen\_Default: \mathbb{P}\ (DETEKTOR \times \mathbb{N})$
$Soundeinstellung\_Default: \mathrm{P}\ (DETEKTOR \times STATUS)$
$Detektortypen: \mathrm{P}\ (DETEKTOR \times DETEKTORTYP)$
$xcontrol\_startup: XCONTROLSTARTUP$
$default\_balkenanzahl: \mathbb{N}$
$min\_zeitbegrenzung, max\_zeitbegrenzung: HUNDERTSTEL$
$min\_impulsbegrenzung, max\_impulsbegrenzung: \mathbb{N}$
$min\_intensitaetsbegrenzung, max\_intensitaetsbegrenzung: \mathbb{N}$

Zählerfenster – Systemzustand

XCTL

INI_File
zaehlerfenster, konfigurationsfenster: STATUS
Aktive_Detektoren: $\mathbb{P}$ *DETEKTOR*
sound: STATUS
anzeige: ANZEIGE
aktueller_detektor: DETEKTOR
aktuelle_zeitbegrenzung, sicherung_zeitbegrenzung: HUNDERTSTEL
aktuelle_impulsbegrenzung: $\mathbb{N}$

Zählerfenster – Systemzustand

Anzeige_Zaehlerfenster

$$
\begin{array}{l}
XCTL \\
aktuelle\_intensitaet, default\_intensitaet, min\_intensitaet, max\_intensitaet, \\
aktuelle\_balkenanzahl, min\_balkenanzahl, max\_balkenanzahl: \mathbb{N} \\
anzeigeeinstellung, log\_datei, pop\_up\_menu: STATUS
\end{array}
$$

Zaehler

$$
\begin{array}{l}
XCTL \\
Zeit \\
aktueller\_wert: \mathbb{N} \\
beginn\_zaehlung : HUNDERTSTEL \\
\hline
t - beginn\_zaehlung \leqslant aktuelle\_zeitbegrenzung \\
aktueller\_wert \leqslant aktuelle\_impulsbegrenzung
\end{array}
$$

Formale Spezifikation in Reverse-Engineering-Prozessen für technische Systeme

Zählerfenster – Initialzustand

Init_XCTL

INI_File
XCTL'
Anzeige_Zaehlerfenster'
Zaehler'
ΔZeit

$\forall x:\mathbb{N}$
• *detektor* $x \in$ *Aktive_Detektoren'*
$\Leftrightarrow x = 0 \lor (\exists y:\mathbb{N} \mid$ *detektor* $y \in$ *Aktive_Detektoren'* • $x - y = 1)$
Aktive_Detektoren' $\neq \varnothing$
zaehlerfenster' = *Aus* $\Leftrightarrow$ *xcontrol_startup* = *Startup_Nothing*
zaehlerfenster' = *Ein* $\land$ *Init_Anzeige_Zaehlerfenster* $\land$ *Init_Zaehler*
$\Leftrightarrow \neg$ *xcontrol_startup* = *Startup_Nothing*
konfigurationsfenster' = *Aus*
aktueller_detektor' = *detektor* 0
$\exists z:$ *DETEKTOR* x *HUNDERTSTEL* |
$z \in$ *Zeitbegrenzungen_Default* $\land z.1 =$ *detektor* 0 • *aktuelle_zeitbegrenzung'* = $z.2$
$\exists i:$ *DETEKTOR* $\times \mathbb{N} \mid i \in$ *Impulsbegrenzungen_Default* $\land i.1 =$ *detektor* 0
• *aktuelle_impulsbegrenzung'* = $i.2$
$\exists s:$ *DETEKTOR* $\times$ *STATUS* $\mid s \in$ *Soundeinstellung_Default* $\land s.1 =$ *detektor* 0
• *sound'* = $s.2$
$t' = 0$

Zählerfenster – Initialzustand

Init_Anzeige_Zaehlerfenster

$Anzeige\_Zaehlerfenster'$

$aktuelle\_intensitaet' = 140001$
$default\_intensitaet' = 260000$
$min\_intensitaet' = min\_balkenanzahl' = 0$
$max\_intensitaet' = 2000000$
$max\_balkenanzahl' = 140$
$log\_datei' = Aus$

Init_Zaehler

$Zaehler'$
$\Xi Zeit$

$beginn\_zaehlung' = t$
$aktueller\_wert' = 0$

Zählerfenster – Operationen

→ insgesamt 18 Operationen identifiziert

- Einblenden/Ausblenden des Konfigurationsfensters
- Aktivieren/Deaktivieren der Speicherung von Messdaten
- Ändern der Anzeige
- Einblenden/Ausblenden und Ändern der Anzeigeeinstellungen
- Änderung der Soundoption
- Änderung der aktuellen Zeitbegrenzung
- Änderung der aktuellen Impulsbegrenzung
- Einblenden/Ausblenden des Zählerfensters
- Detektorauswahl
- Zählvorgang
- Zählerneustart (zeit- und impulsbedingt)
- Beenden von XCTL

Zählerfenster – Zeitaspekt

→ Einfaches Zeitmodell aus „Z and the Specification of Real-Time Systems" von J-M.Bruel, A.Benzekri, Y.Raynand

$$HUNDERTSTEL == \mathbb{N}$$

Zeit

$$t : HUNDERTSTEL$$

Tick

$$\Delta Zeit$$

$$t' = t + 1$$

Zählerfenster – Operationen

→ Beispiel: Zählerneustart

Zaehler_Neustart_Zeitbedingt

$\Delta Zaehler$
$\Xi Zeit$
$output!: \mathbb{N}$
$z: DETEKTOR \times \mathbb{N}$

$t - beginn\_zaehlung > aktuelle\_zeitbegrenzung$
$aktueller\_wert' = 0$
$beginn\_zaehlung' = t$
$output! = aktueller\_wert$
$aktuelle\_zeitbegrenzung' = sicherung\_zeitbegrenzung$

Zählerfenster – Zeitaspekt

→Beispiel: Zählerneustart

Zaehler_Neustart_Impulsbedingt

$\Delta Zaehler$
$\Xi Zeit$
$output!: \mathbb{N}$

$aktueller\_wert > aktuelle\_impulsbegrenzung$
$output! = aktueller\_wert$
$aktuelle\_zeitbegrenzung' = aktuelle\_zeitbegrenzung - (t - beginn\_zaehlung)$
$\wedge\ beginn\_zaehlung' = t$
$aktueller\_wert' = 0$

Probleme der verbalen Spezifikation

Manuelle Justage (Alt):

- fünf Probleme in verbaler Beschreibung identifiziert

0-dim. Detektoren, Teilfunktion Zählerfenster:

- keine Probleme festgestellt
- Diskussion des erstmaligen Starts des Zählers

Probleme der verbalen Spezifikation

Manuelle Justage (Alt) – Beispiel 1: Bewegungsgeschwindigkeit

Beschreibung aus dem Pflichtenheft:

„… *Im Schrittbetrieb wird der Antrieb immer mit der maximal möglichen Geschwindigkeit bewegt….*“

→ Fehler – Die Geschwindigkeit im Schrittbetrieb ist nicht immer maximal.

- Schrittbetrieb ist aktiviert
- Veränderung des Geschwindigkeitswertes hat Auswirkung Schrittbetrieb
- Bewegung im Schrittbetrieb erfolgt mit aktueller Geschwindigkeit

Probleme der verbalen Spezifikation

Manuelle Justage (Alt) – Beispiel 2:

Punkt 2.3e Reaktion auf unzulässige Eingaben, 3. unzulässige Schrittweite

Beschreibung aus dem Pflichtenheft

„*…Falls durch die Nutzung einer zulässigen Schrittweite der Bereich für zulässige Winkelpositionen verlassen wird, muss ebenfalls eine Korrektur der Schrittweite vorgenommen werden.*“

→ Ungenauigkeit

- Systemverhalten wird nicht beschrieben
- Beobachtung: würde eine Schritt die Positionsgrenzen überschreiten, geschieht nichts

Probleme der verbalen Spezifikation

0-dim. Detektoren, Teilfunktion Zählerfenster

Diskussion: erstmaliger Start des Zählers

Beschreibung aus dem Pflichtenheft

„Ist der Startup-Parameter nicht entsprechend gesetzt und damit auch kein Zählvorgang nach dem Programmstart gestartet worden, erfolgt der Start des Zählvorganges bei der erstmaligen Wahl der Hauptmenüfunktion: Einstellungen > Detektoren > Detektoren ...
Gestartet wird der erste verfügbare Detektor, der in der Dialogbox auch angezeigt wird (s. Pkt. 2.3.1.a). Ist zusätzlich der Sound-Parameter in dem entsprechenden Device-Abschnitt gesetzt, erfolgt außerdem eine von den Zählraten abhängige akustische Ausgabe (s. Pkt. 2.3.1.d). Das Zählerfenster wird nicht automatisch geöffnet, sondern erst nach dem Setzen des Markierungs-Feldes Fenster > Anzeigen (s. Pkt. 2.3.1.c).“

Probleme der verbalen Spezifikation

0-dim. Detektoren, Teilfunktion Zählerfenster

Diskussion: erstmaliger Start des Zählers

Annahme: Soundparameter ist nicht gesetzt

→ Keine optische oder akustische Ausgabe der Zählrate
→ Messdaten Speichern ist deaktiviert

Woher weiß man, ob der Zählvorgang gestartet wurde?

Auswertung & Ausblick

- zwei formale Verhaltensspezifikationen sind entstanden
- Probleme in verbaler Beschreibung identifiziert
- Pflichtenheft von Manuelle Justage (Alt) erweitert (farbliche Hervorhebung von Fehlern, Ungenauigkeiten, Beobachtungen)

- Einsatz der Z-Notation weiterführen
- weitere Teilsysteme formal Beschreiben
- Review der erstellten formalen Spezifikationen