

Der Zufallsapparat 15a
Versuch 01
Die Digitalschaltungen im CPLD
Kurzbeschreibung
10. 9. 2015

Zweck:

Vorerprobung zur Nutzung von Komparatoren als Entropiequelle. Das Verfahren beruht darauf, daß Komparatoren ins Schwingen geraten können, wenn die Differenzspannung zwischen beiden Eingängen in der Größenordnung der Eingangsoffsetspannung liegt. Dieser Betriebszustand wird zeitweise zyklisch herbeigeführt. Dabei wird das Schwingungsverhalten ausgewertet. Es gibt Schwingungsverläufe, die zur Gewinnung von Zufallszahlen geeignet sind und solche, die dazu nicht geeignet sind. Die ersten Versuche betreffen das Zählen der Impulse und das Auszählen der Impulsbreiten.

Versuch 01: Impulszählung

Die CPLD enthält 4 Zähleraltungen, deren Takteingänge an die Komparatorausgänge angeschlossen sind. Jede Zähleraltung besteht aus einem 8-Bit-Binärzähler mit beschränkter Zählweite und einem 2-Bit-Binärzähler ohne Zählweitenbeschränkung (Hilfszähler).

Zähltakt

Vom Komparatorausgang ohne jede weitere Aufbereitung.

Zählweitenbeschränkung

Durch Decodieren der Endstellung (FFH). Ist diese Stellung erreicht, wird nicht mehr weitergezählt. Das decodierte Signal wirkt invertiert auf den Zählerlaubnis Eingang (Count Enable CE).

Zählwertausgabe (1)

Über den 8-Bit-Bus. Es gibt 5 Auswahlmöglichkeiten: jeweils einen der 4 8-Bit-Zähler sowie alle 4 2-Bit-Zähler (Hilfszähler) parallel.

Zählwertausgabe (2)

Die 4 2-Bit-Zähler (Hilfszähler) sind invertiert nach außen geführt. Nutzung: zum Anschließen von LEDs (Balkenanzeige der Versuchsplatine 15a).

Löschen der Zähler

Durch Schreiben eines Bytes über den Datenbus. Die 8-Bit-Zähler sind einzeln löscherbar, die 2-Bit-Zähler (Hilfszähler) gemeinsam.

Die Nutzung der beiden Zählerarten

In diesem Versuch ist zunächst vorgesehen, je Durchlauf und Komparator nur ein einziges Zufallsbit zu gewinnen (Prinzip Münzenwurf oder Würfeln Gerade / Ungerade). Es kann vorkommen, daß der Komparator sehr viele Impulse abgibt. Das sollte erkennbar sein, deshalb sollte der Zähler nicht überlaufen. Wird der Zählwert FFH ausgelesen, so sind 255 oder mehr Impulse eingelaufen. In einer ersten Versuchsvariante kann man einen solchen Durchlauf als

unbrauchbar verwerfen. Es sollte aber auch alternativ möglich sein, längere Impulsfolgen oder Impulse aus anderen Ursachen¹ versuchsweise als Entropiequelle auszunutzen. Hierzu wurden die Hilfszähler vorgesehen, die bei beliebig langen Impulsfolgen auf jeden Fall eine Entscheidung Gerade / Ungerade zulassen. Die zusätzliche LED-Anzeige dieser Zählwerte ermöglicht zudem eine pauschale visuelle Kontrolle.

Die CPLD aus Sicht des Mikrocontrollers

Bus:

7	6	5	4	3	2	1	0
XBUS7	XBUS6	XBUS5	XBUS4	XBUS3	XBUS2	XBUS1	XBUS0

Steuersignale:

7	6	5	4	3	2	1	0
ENABLE	SEL_2	SEL_1	SEL_0	–	–	–	–

Busbelegung beim Lesen der Hilfszähler:

7	6	5	4	3	2	1	0
Hilfszähler 3, Bit B	Hilfszähler 3, Bit A	Hilfszähler 2, Bit B	Hilfszähler 2, Bit A	Hilfszähler 1, Bit B	Hilfszähler 1, Bit A	Hilfszähler 0, Bit B	Hilfszähler 0, Bit A

Busbelegung zum Löschen der Zähler:

7	6	5	4	3	2	1	0
–	–	–	Löschen Hilfszähler (alle)	Löschen Zähler 3	Löschen Zähler 2	Löschen Zähler 1	Löschen Zähler 0

Die Auswahlsignale SEL2..0:

SEL2...0	Funktion	Wirkung
0	Lesen Zähler 0	Lesen, CPLD treibt. Inhalt von Zähler 0 auf Bus.
1	Lesen Zähler 1	Lesen, CPLD treibt. Inhalt von Zähler 1 auf Bus.
2	Lesen Zähler 2	Lesen, CPLD treibt. Inhalt von Zähler 2 auf Bus.
3	Lesen Zähler 3	Lesen, CPLD treibt. Inhalt von Zähler 3 auf Bus.
4	Lesen Hilfszähler	Lesen, CPLD treibt. Inhalte der Hilfszähler auf Bus.
5	–	Lesen, CPLD treibt.
6	–	Lesen, CPLD treibt.
7	Zähler löschen	Schreiben, Mikrocontroller treibt. Löschststeuerbits auf Bus.

1: Dem Prinzip nach gibt ein Komparator nur dann Impulse ab, wenn die Differenzspannung über seinen Eingängen den linearen Bereich durchläuft. Infolge von gegenseitigen Beeinflussungen, Störeinkopplungen usw. können aber auch außerhalb dieser Zeitabschnitte Impulse auftreten.

Das Businterface arbeitet nach dem Prinzip der Motorola-Signalisierung (ähnlich vielen typischen LCD-Anzeigen). ENABLE ist das Zugriffserlaubnissignal (vgl. das Signale E der LCD-Anzeigen). Das Bitmuster der Auswahlensignale (SEL0, 1, 2) bestimmt sowohl die Zugriffsauswahl (Registeradresse) als auch die Datenflußrichtung (Lesen oder Schreiben).

Die Zugriffe aus Sicht des Mikrocontrollers

Ruhezustand:

ENABLE = Low. SEL2...0 gleichgültig. Bus in Ruhe (Eingabe mit Pullups oder Ausgabe).

Lesen:

1. Den Bus auf Eingabe schalten.
2. Den Auswahlcode auf SEL2...0 legen.
3. ENABLE auf High.
4. Synchronisationszeit abwarten (gemäß Datenblatt Mikrocontroller).
5. Den Bus einlesen.
6. ENABLE auf Low.
7. Den Bus auf Ruhezustand schalten (Eingabe mit Pullups oder Ausgabe).

Schreiben:

1. Den Auswahlcode auf SEL2...0 legen. Damit bleibt der Busanschluß im CPLD hochohmig, auch bei aktivem ENABLE (Schreibzugriff).
2. Den Bus auf Ausgabe schalten.
3. Das Ausgabebitmuster auf den Bus legen.
4. ENABLE auf High.
5. ENABLE auf Low.
6. Den Bus auf Ruhezustand schalten (Eingabe mit Pullups oder Ausgabe).

Zeitbedingungen:

Die CPLD ist grundsätzlich schneller als der Mikrocontroller. Sie kann mit lückenlosen Befehlsfolgen (ohne Wartezeiten) angesteuert werden mit der Ausnahme des Synchronisierens beim Lesen (s. Schritt 5 des Leseablaufs).

Überblick über den Schaltplan

Blatt 1

Die 4 8-Bit-Zähler. Takteingänge von den Komparatoren.

Blatt 2 bis 5

Lesedatenauswahl. 8-Bit-Zähler über Multiplexer 4 zu 1, Hilfszählerauswahl über nachgeschaltete Multiplexer 2 zu 1.

Blatt 6

Zählweitenbeschränkung und Löschen der 8-Bit-Zähler. Zählerlaubnis wird inaktiv (INHIB-Signal), wenn Zählerstand = FFH. Löschen (CLR-Signal) mit ENABLE bei SELECT2..0 auf Löschfunktion (CLEAR_CTR) und betreffendem Bussignal = High.

Blatt 7

Bus. Außen bidirektional (XBUS), innen zwei Datenwege, einer zur Eingabe, einer zur Ausgabe. Aufschaltung der Ausgabedaten (BUS_OUT), wenn GTS_IN auf Low (Tristate-Signal). Ausgabe = Lesen. Bus wird getrieben. Eingabe = Schreiben. Bus wird nicht getrieben (hochohmig, Tristate).

Die Signale SEL0 bis SEL2 und ENABLE.

Decodierung Löscherlaubnis (CLEAR_CTR = alleSEL-Signale High).

Decodierung Busaufschaltung (Ausgabe). Der Bus ist immer hochohmig (GTS_OUT auf High), wenn ENABLE inaktiv ist oder wenn ein Schreibzugriff zum Löschen erfolgt.

$$\begin{aligned} \text{GTS_OUT} &= \overline{\text{ENABLE}} \vee \text{CLEAR_CTR} \\ &= \overline{\text{ENABLE} \cdot \overline{\text{CLEAR_CTR}}} \end{aligned}$$

Blatt 8 und 9

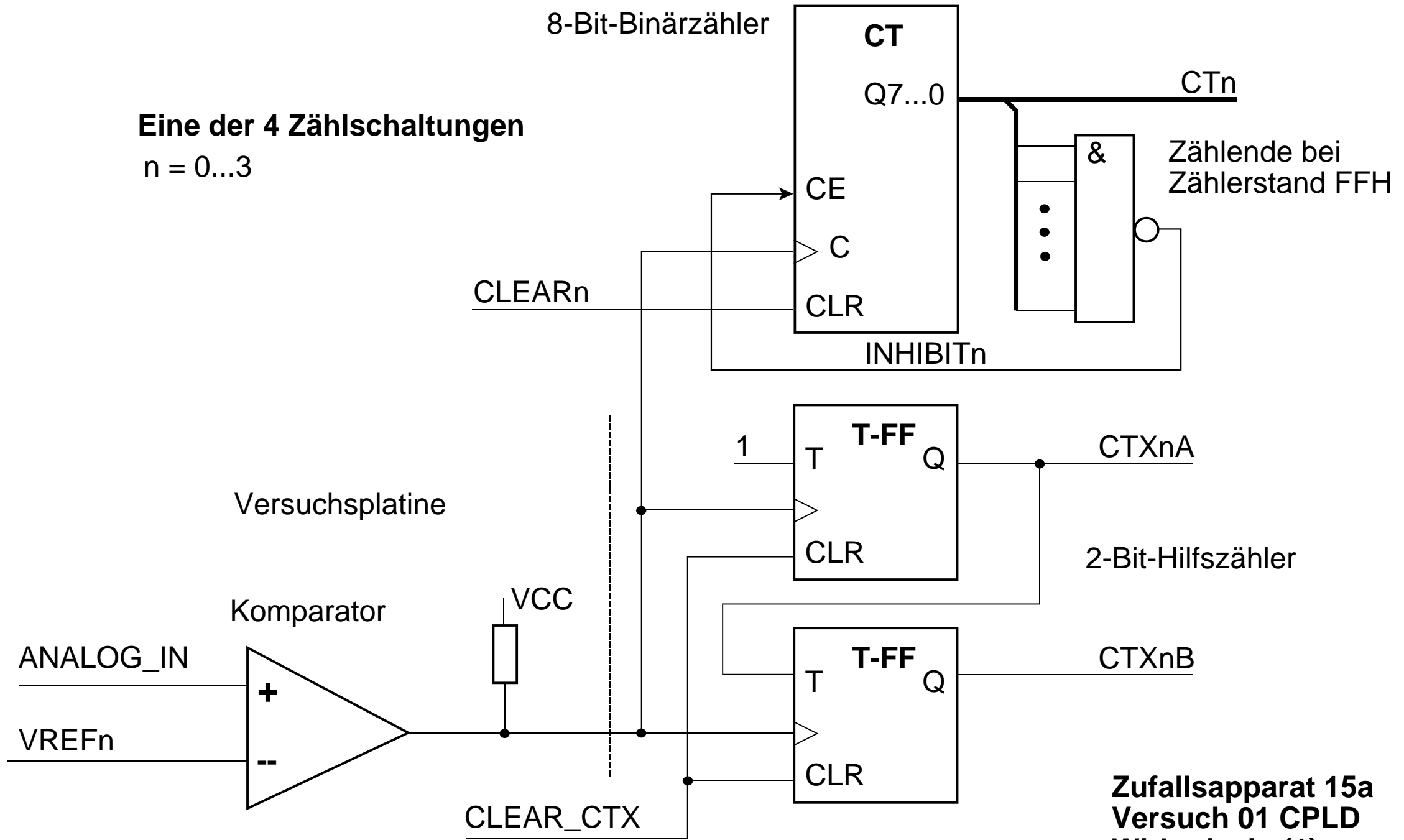
Die 2-Bit-Hilfszähler

Blatt 10

Die invertierte Ausgabe der Hilfszähler (zwecks LED-Anzeige).

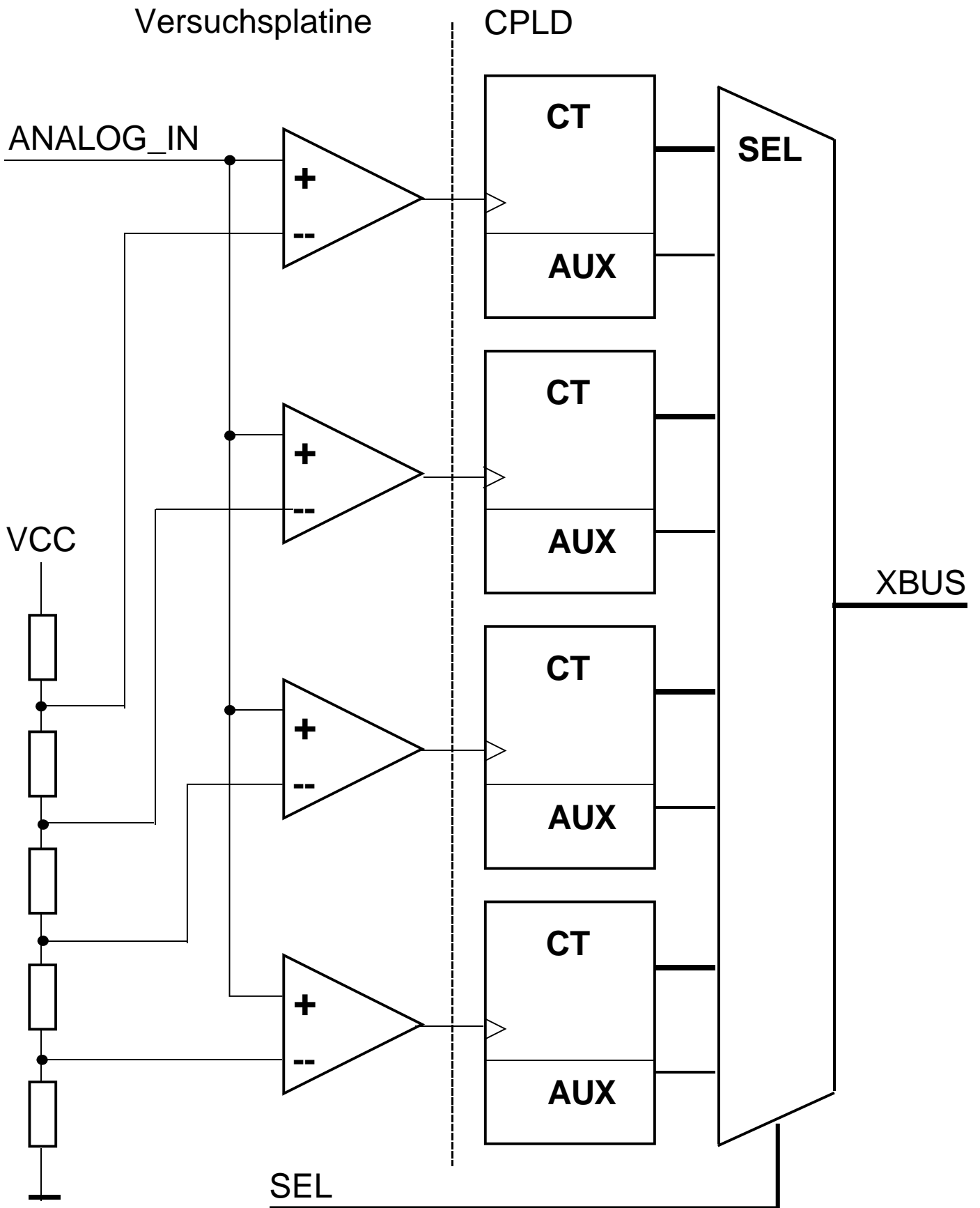
Die Decodierung des Hilfszählerlöschssignals (CTXCLEAR). Es wird aktiv, wenn beim Löschen der Zähler (CLEAR_CTR und ENABLE) das Bit 4 der Buseingabe (BUS_IN(4)) High ist.

Die Decodierung der Hilfszählerauswahl. Lesen der Hilfszähler mit SEL2, 1, 0 = 4 = 100B (s. Tabelle).



Eine der 4 Zählschaltungen
n = 0...3

Zufallsapparat 15a
Versuch 01 CPLD
Wirkprinzip (1)
11. 9. 2015



Prinzip der Zählwertausgabe

**Zufallsapparat 15a
 Versuch 01 CPLD
 Wirkprinzip (2)
 26. 6. 2015**