Zufallsapparat 15a
Versuchsprogramm Xmega V01
Kurzbeschreibung

14. 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.

Versuch V01 betrifft das Zählen der Impulse (Impulsanzahlbewertung).

Plattform:
Zufallsapparat 15a mit CPLD Xilinx 9572 PLCC 44, Versuch 01.

Bedienung und Anzeige:

a) über Einheitsbedientafel 02/10 (Elementarbedienung),

b) über serielle Schnittstelle und Terminalprogramm auf PC,

c) über serielle Schnittstelle und Sonderbedienprogramm auf PC.

Initialisierung:
Ausgabe des Analogwertes 0, Abfrage und Anzeige aller Zählerinhalte, Anzeige des aktuellen Analogwerts.

Ruhezustand:
Warten auf Bedienhandlungen oder serielle Kommandos (Grundsteuerschleife / Tastenschleife).

Bedienmöglichkeiten über Einheitsbedientafel 02/10 (Elementarbedienung):

1. Inkrementalgeber: Statische Analogwerteingabe.

2. CANCEL: Den statischen Analogwert auf 0 setzen und die Zahlenwurmanzeige löschen.

3. ENTER: Die Anfangs- und Endwerte der Analogsignalbereiche bestimmen und anzeigen.

4. UP: Den Algorithmus auswählen (Strategienummer; Weitertasten in Richtung Anfang (Dekrement)).

5. DOWN: Den Algorithmus auswählen (Strategienummer; Weitertasten in Richtung Ende (Inkrement)).

6. LEFT: Die Zufallszahlenerzeugung einmal ausführen.

7. RIGHT: Die Zufallszahlenerzeugung solange ausführen, wie die Taste niedergehalten wird.

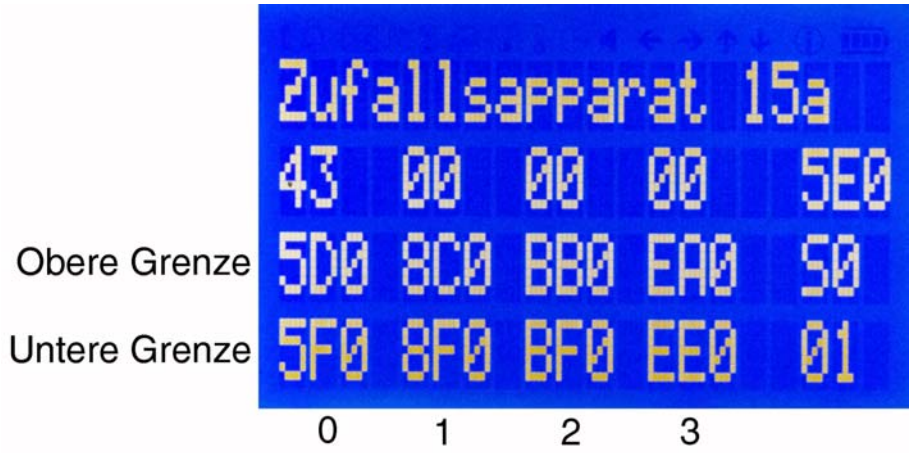
Zufallszahlenausgabe während der Elementarbedienung:
Die Zufallszahlen werden Bit für Bit gebildet. Je Bit wird ein Zeichen (0 oder 1) abgegeben. Diese Bitzeichen werden über die serielle Schnitsttelle gesendet und auf der LCD-Anzeige dargestellt (Zahlenwurmanzeige). Die aktuellen Bitzeichen erscheinen jeweils rechts außen.

Fehlstellenkennzeichnung:
Ein Zufallsbit wird nur dann gebildet, wenn der jeweilige Zählwert bestimmte Bedingungen erfüllt. Bei Nichterfüllung ergibt sich eine sog. Fehlstelle. Ist die Fehlstellenkennzeichung aktiv, wird anstelle eines Zufallsbitzeichens (0 oder 1) ein Zeichen X abgegeben. Ist die Fehlstellenkennzeichnung nicht aktiv, wird gar kein Bitzeichen abgegeben. Es erscheinen dann beispielsweise statt 4 nur 3 Zufallsbitzeichen.

Die Anzeige nach dem Einschalten oder Hardware-Rücksetzen:

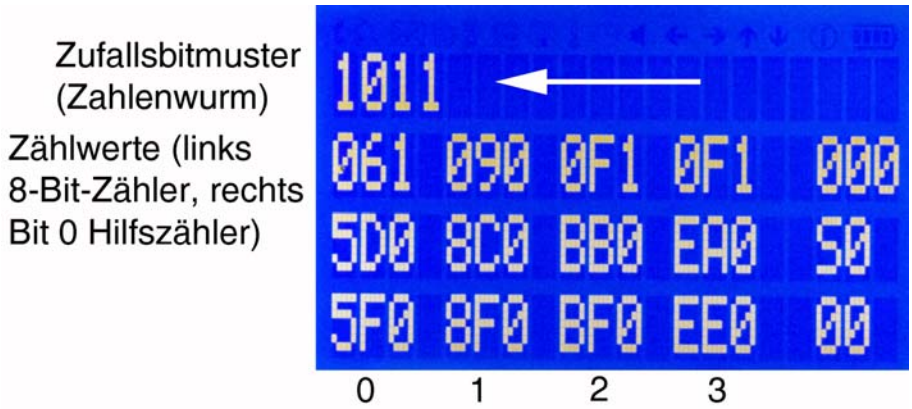
Mit dem Inkrementalgeber wurde ein Analogwert eingedreht. Die Zählerstände, die sich danach ergeben haben, werden angezeigt:

Die ENTER-Taste wurde betätigt. Die Analogsignalbereiche werden angezeigt:



Die Wirkung der CANCEL-Taste. Gelöscht werden: 1. die oberste Zeile (= Begrüßungstext oder Zufallszahlen) und 2. der Analogwert. Die Zählerstände bei Analogwert 0 werden angezeigt:

Betätigung der LEFT-Taste. Die Zufallszahlenerzeugung wird einmal durchlaufen. Es werden 4 Zufallsbits gebildet:



Laufende Zufallszahlenerzeugung. Anzeige in der obersten Zeile. Die jeweils aktuellen Bits werden vom rechten Rand an eingeschoben (Zahlenwurm). Tasten LEFT (einmalig; mit Fehlstellenanzeige) oder RIGHT (Durchlauf, solange Taste niedergehalten; mit Fehlstellenanzeige). X = Fehlstelle (infolge des Zählerstandes keine Zufallsbitbildung möglich):

Zufallszahlenanzeige ohne Fehlstellen. Nur Nullen und Einsen:

Algorithmenauswahl mit den Tasten UP und DOWN. Zyklisches Weiterschalten. Hier ist Strategie S2 ausgewählt:

Der Aufbau der Strategienummer (0...F; her nur 0...B implementiert)

3	2	1	0
Algorithmus		Fehlstellenanzeige	Zählerauswertung

Algorithmenauswahl

Strategie	**Funktion**	**Fehlstellenanzeige**	**Zählerauswertung**
0	Bereichsweiser Durchlauf	Nein	Hilfszähler
1	Bereichsweiser Durchlauf	Nein	Zählerstand
2	Bereichsweiser Durchlauf	Ja	Hilfszähler
3	Bereichsweiser Durchlauf	Ja	Zählerstand
4	Kontinuierlicher Durchlauf	Nein	Hilfszähler
5	Kontinuierlicher Durchlauf	Nein	Zählerstand
6	Kontinuierlicher Durchlauf	Ja	Hilfszähler
7	Kontinuierlicher Durchlauf	Ja	Zählerstand
8	Kontinuierlicher Durchlauf, 2 Richtungen	Nein	Hilfszähler
9	Kontinuierlicher Durchlauf, 2 Richtungen	Nein	Zählerstand
A	Kontinuierlicher Durchlauf, 2 Richtungen	Ja	Hilfszähler
B	Kontinuierlicher Durchlauf, 2 Richtungen	Ja	Zählerstand

Zählerauswertung:

- Hilfszählerauswertung. Bedingung: Zählwert (des 8-Bit-Zählers) ≥ Minimum. Das Maximum wird nicht ausgewertet. Es können mehr als 255 Schwingungen aufgetreten sein (Zählweitenbegrenzung im CPLD). Zufallsbit = Hilfszählerstelle 0 (Gerade/Ungerade).
- Zählerstandauswertung. Bedingung: Minimum ≤ Zählwert ≤ Maximum = FFH (Zählweitenbegrenzung im CPLD). Zufallsbit = Zählerstelle 0 (Gerade/Ungerade).

Programmkomponenten

tastenschleife:
Tastenabfrage. Hauptsteuerschleife.

Analogwertanzeige Inkrementalgeber
Der Geber stellt den Analogwert ein. Die Zähler werden gelöscht. Danach wird der Analogpegel ausgegeben. Nach Ablauf der zugehörigen Wartezeit (vinspect_settling_time) werden die Zähler eingelesen und angezeigt.

step1:
Die Anfangs- und Endwerte der Vergleichsbereiche gewinnen (Kalibrierung).

sample_once:
Einen einzelnen Durchlauf ausführen. Verzweigen gemäß Strategieauswahl:

- 0 bis 3: Bereichsweiser Durchlauf (Treppenspannung).
- 4 bis 7: Kontinuierlicher Durchlauf (Sägezahnspannung).
- 8 bis B: Kontinuierlicher Durchlauf in 2 Richtungen (Dreieckspannung).

Macro scan_voltage_window:
1. Den Analogwert anbieten.
2. Die Verweilzeit abwarten.
3. Hat der betreffende Zähler gezählt?
4. Wenn nicht, ist der Pegel noch zu niedrig. Erhöhen und wiederholen.
5. Wenn ja, ist die Anzahl an gezählten Impulsen ausreichend?
6. Wenn nein, dann den Pegel erhöhen und wiederholen.
7. Wenn ja, ist der Anfangswert gefunden. Er wird um 1 vermindert gespeichert.
8. Dann wird nach dem Ende des Bereichs gesucht. Dazu den nächsten Analogwert anbieten.
9. Kommen noch Impulse?
10. Wenn ja, dann Pegel erhöhen und weiter probieren.
11. Wenn nein, ist der Endwert gefunden. Er wird gespeichert.

Macro sample_window:
1. Den Analogwert anbieten.
2. Die Verweilzeit abwarten.
3. Solange wiederholen, bis der gesamte Bereich vom Anfangswert bis zum Endwert durchlaufen ist.
4. Dann die Zählwerte (Zähler + Hilfszähler) abholen.

Der einfachste kontinuierliche Durchlauf (primitivschleife):
1. Der erste Analogwert ist 0.
2. Den Analogwert anbieten.
3. Die Beruhigungszeit abwarten.
4. Bis zum letzten Analogwert (4095) wiederholen.
5. Dann alle Zähler auslesen.

Ablaufparameter:

Name*	Bedeutung	Länge (Bits)
vcal_entry_settling_time, cal_entry_settling_time	Wartezeit beim Kalibrieren auf das Eintreffen von Impulsen (Komparator soll schwingen)	16
vcal_exit_settling_time, cal_exit_settling_time	Wartezeit beim Kalibrieren auf das Ausbleiben von Impulsen (Komparator soll nicht mehr schwingen)	16
vscan_settling_time, scan_settling_time	Wartezeit bei der Zufallszahlengewinnung	16
vinspect_settling_time, inspect_settling_time	Wartezeit beim Eindrehen eines einzelnen Analogwertes	16
vsimple_settling_time, simple_settling_time	Wartezeit bei der Zufallszahlengewinnung mit kontinuierlichem Durchlauf	16
vminimum_cal_count, minimum_cal_count	Mindestimpulsanzahl beim Kalibirieren	8
vminimum_scan_count, minimum_scan_count	Mindestimpulsanzahl bei der Zufallszahlengewinnung	8
vcal_step, cal_step	Schrittweite Analogwert beim Kalibirieren	8
vscan_step, scan_step	Schrittweite Analogwert bei der Zufallszahlengewinnung	8
vsimple_step, simple_step	Schrittweite Analogwert bei der Zufallszahlengewinnung mit kontinuierlichem Durchlauf	8
vincremental_step, incremental_step	Schrittweite Analogwert beim Eindrehen mit Inkrementalgeber	8

*: 1. Wert: Variable. Auch über serielle Schnittstelle zu beeinflussen. 2. Wert: Festwert nach dem Einschalten. Zeiten in µs.

Alle Parameter sind variabel. Sie stehen im RAM und können über serielle Kommandos verändert werden. Nach dem Einschalten werden zunächst Festwerte aus dem Programmspeicher des Mikrocontrollers geladen.

Die Analogwerte der Vergleichsfenster
16 Bits Speicherung, 12 Bits Zahlenwerte

analog_windows:

Anfangswert für VREF0
Endwert für VREF0
Anfangswert für VREF1
Endwert für VREF1
Anfangswert für VREF2
Endwert für VREF2
Anfangswert für VREF3
Endwert für VREF3

Die Zählergebnisse
8 Bits

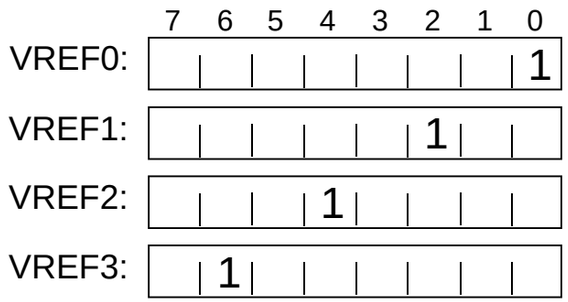
analog_samples:

VREF0 Zählwert
VREF0 Hilfszählerbit
VREF1 Zählwert
VREF1 Hilfszählerbit
VREF2 Zählwert
VREF2 Hilfszählerbit
VREF3 Zählwert
VREF3 Hilfszählerbit

aux_buffer:

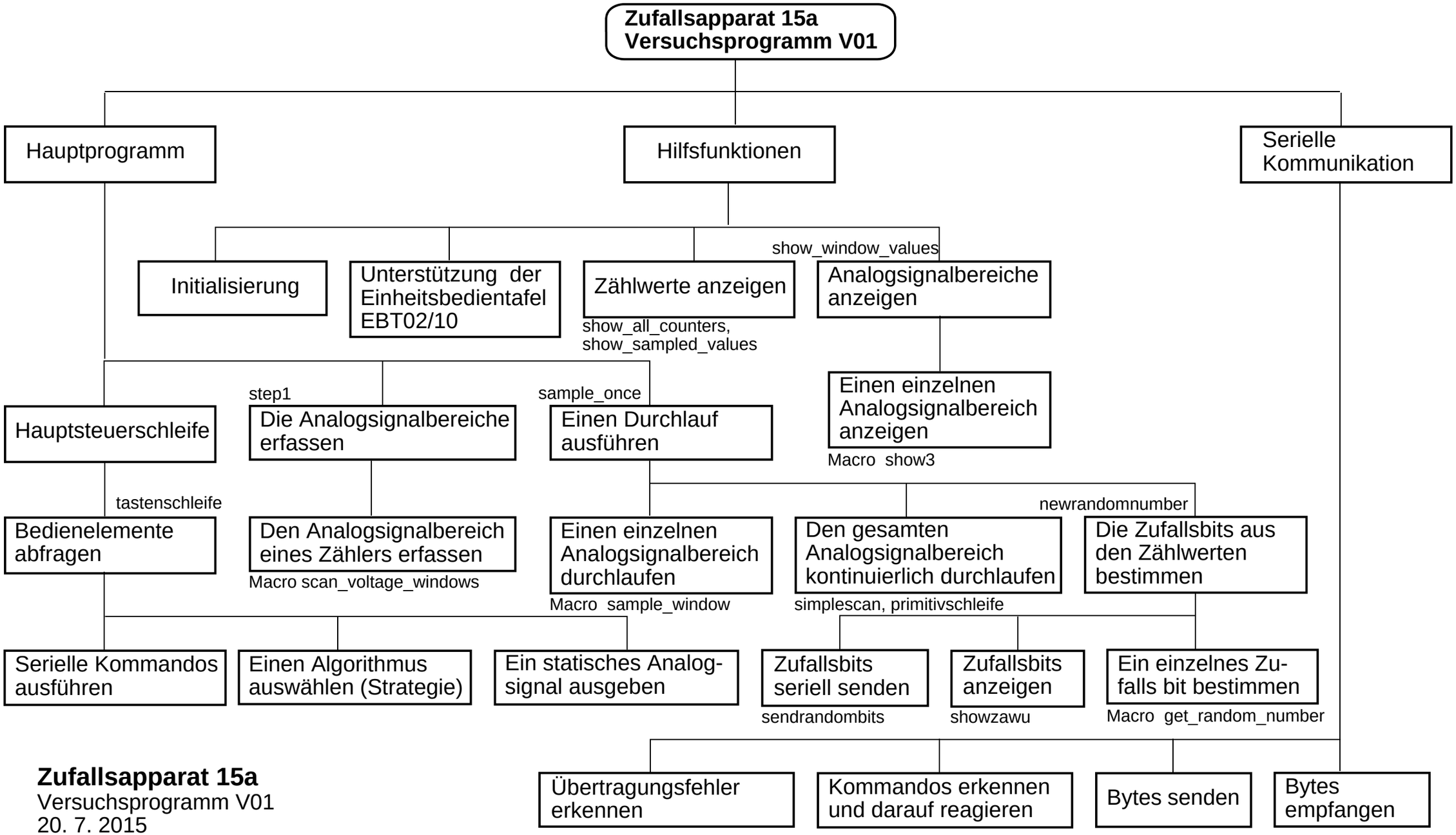
Alle Hilfszählerbits

Die Hilfszählerbits im Block analog_samples:
Es wird nur die Bitposition der betreffenden niederwertigen Hilfszählerstelle (AUX..A) gespeichert.



Zufallsgeneratorprogramm V01

9. 7. 2015



Zufallsapparat 15a
Versuchsprogramm V01
20. 7. 2015