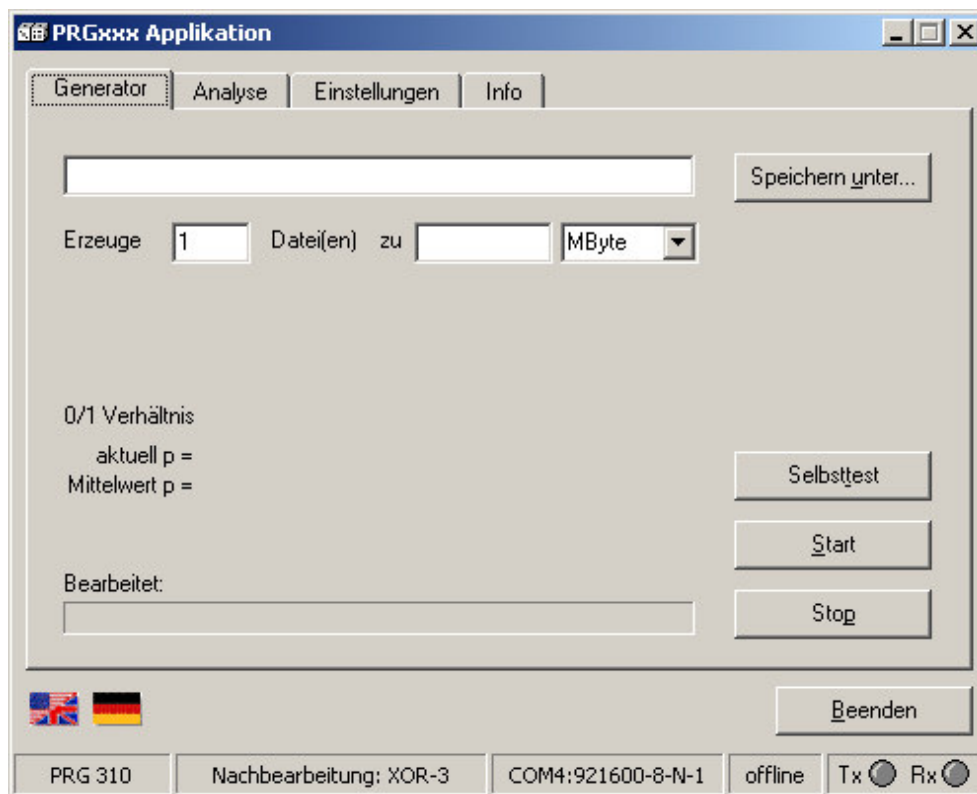


PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Generieren und Analysieren von Zufallszahlen

Software PRG100



Datum: 14.08.2007		1
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Copyright (C) 2007

IBB Ingenieurbüro Bergmann
Karolinenhofweg 18
D-12527 Berlin

Alle Rechte vorbehalten. Kein Teil dieser Dokumentation darf in irgendeiner Form (Fotokopie, Druck oder andere Verfahren) ohne ausdrückliche Genehmigung des Herstellers reproduziert oder unter Verwendung elektronischer Systeme verarbeitet, vervielfältigt oder verbreitet werden.

Haftung

Bei der Erarbeitung dieser Dokumentation wurde größter Wert auf die Vollständigkeit und Richtigkeit des Inhalts gelegt. Es kann dennoch keine Garantie für die Vollständigkeit und Richtigkeit übernommen werden.

Für Hinweise zu dieser Dokumentation sind wir dankbar.

Hotline

Die Hotline des Herstellers erreichen Sie unter 030 65489970.

Warenzeichen

MS Windows ist eingetragenes Warenzeichen der Microsoft Corp.

Datum: 14.08.2007		2
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Inhaltsverzeichnis:

1. Allgemeines.....	4
1. Installation	4
2. Programmaufruf	5
3. Programminformation	5
4. Einstellungen	6
5. Generator	7
6. Analysen.....	9
Entropie	10
Bigramm-Darstellung	11
Monte-Carlo-Darstellung	12
Einfache Darstellung	13

Datum: 14.08.2007		3
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

1. Allgemeines

Diese Software dient der Erfassung und grafischen Auswertung von Zufallszahlen mittels verschiedener Applikationen von Zufallsgeneratoren des IBB. Die statistische Bewertung von Zufallszahlen ist mit den bekannten internationalen Analyseprogrammen (NIST-Test-Suite, Diehard-Test, AIS31-Test, usw.) meist nur mit entsprechenden Fachkenntnissen möglich. Die PRG100-Software visualisiert verschiedene Arten der statistischen Verteilung von Zufallszahlen in einfachen, aussagekräftigen Darstellungen.

1. Installation

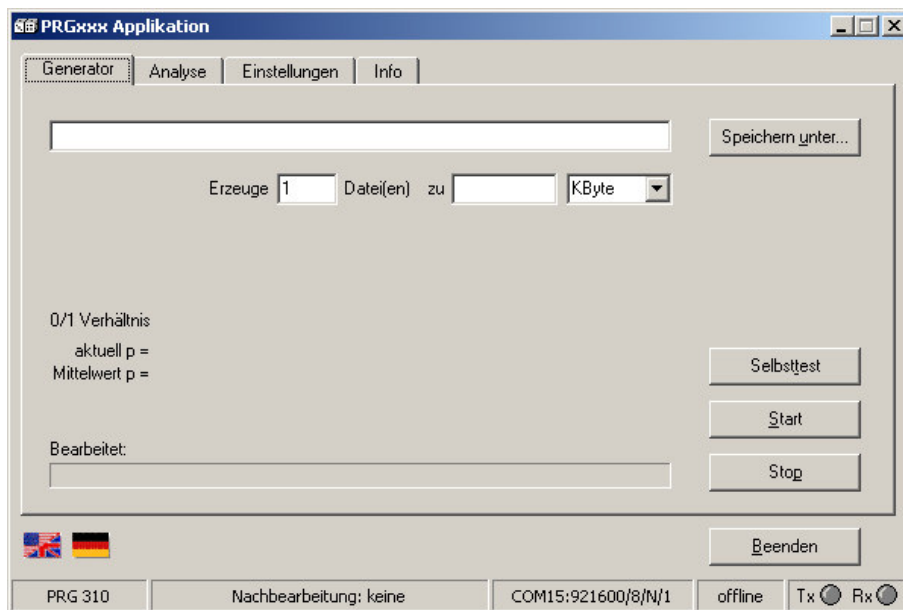
Installieren Sie die auf der CD-ROM befindliche Software durch Aufruf der Datei setup_dt.exe. Die Installation zeigt im angelegten Ordner das Programm PRG100.exe. Eine Deinstallation ist jederzeit möglich.

Datum: 14.08.2007		4
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

2. Programmaufruf

Rufen Sie das Programm durch Doppelklick auf das Symbol der PRG100-Software auf. Es erscheint folgendes Hauptmenü:



3. Programminformation

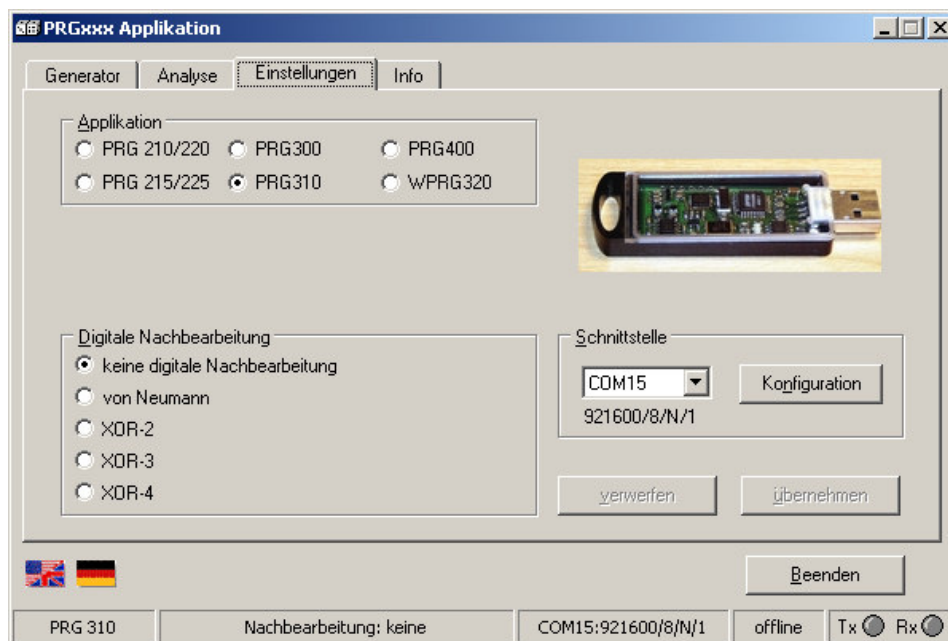


Datum: 14.08.2007		5
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

4. Einstellungen

Falls erforderlich, wählen Sie das Menü „Einstellungen“ aus. Beim Verlassen des Programms werden die aktuellen Einstellungen gespeichert.



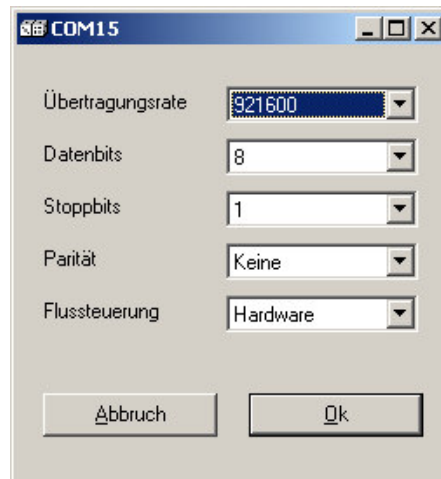
In diesem Menü wählen Sie die am PC angeschlossene Applikation, die Schnittstelle und die gewünschte Nachbearbeitung der generierten Zufallszahlen (hängt von der jeweiligen Applikation ab) aus.

In der Statuszeile (unten) werden die aktuellen Einstellungen abgebildet. Eine Umschaltung zwischen deutscher und englischer Dialogsprache ist in jedem Menü jederzeit möglich.

Datum: 14.08.2007		6
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Die Parameter der Kommunikationsschnittstelle werden dem Handbuch der jeweiligen Applikation entnommen. Hier ein Beispiel für den PRG310-Zufallsgenerator:



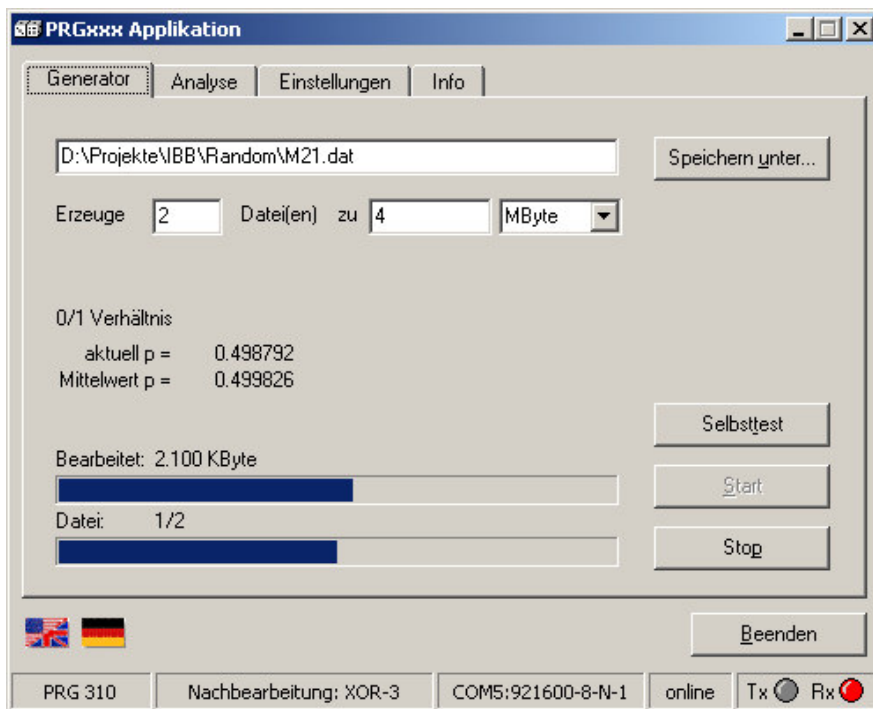
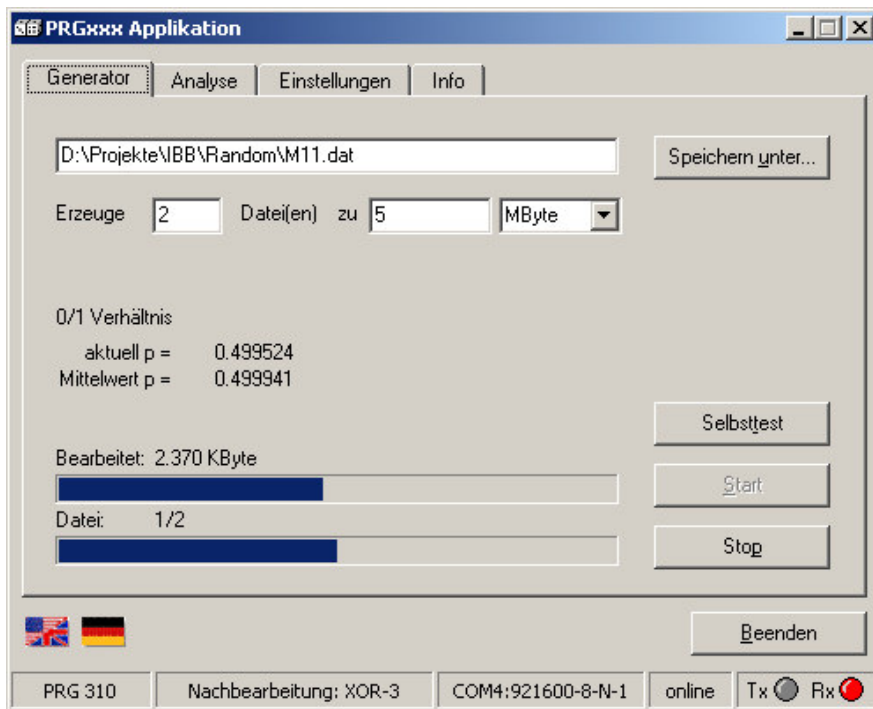
5. Generator

Auf der Seite „Generator“ erfolgt die Generierung der Zufallsdateien. Die Schaltaste „Selbsttest“ bewirkt einen intensiven Test des Zufallsgenerators auf Basis der erzeugten Rohdaten. Die Testparameter sind so eingestellt, dass statistisch 5% aller Tests negativ sein können.

Während der Zufallsgenerierung wird das statistische 0/1-Verhältnis angezeigt. Es können automatisch bis zu 65.500 Dateien in der angegebenen Dateigröße nacheinander erzeugt werden. Es ist möglich, mit bis zu 24 verschiedenen Zufallsgeneratoren (und 24 geöffneten PRG100-Software) unabhängig Zufallsdaten zu erzeugen. Das folgende Beispiel zeigt zwei verschiedene PRG310 (jeweils über COM4 und COM5) bei der Zufallsgenerierung:

Datum: 14.08.2007		7
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

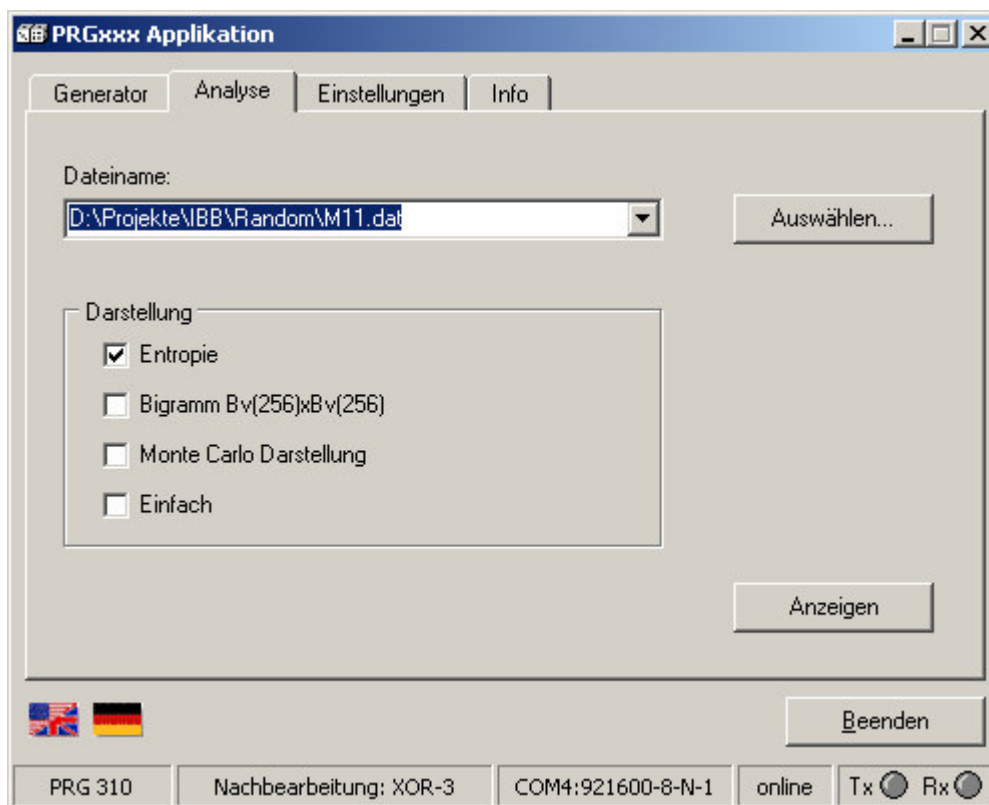


Datum: 14.08.2007		8
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

6. Analysen

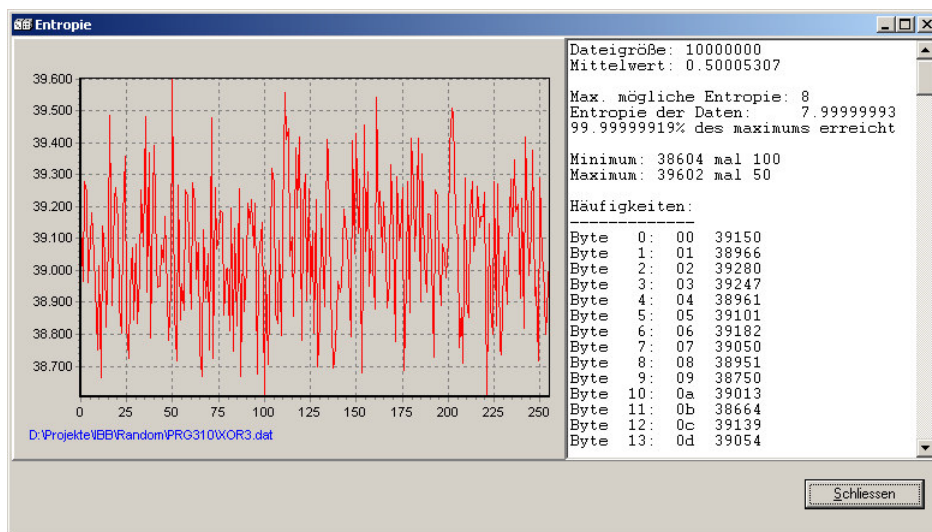
Die Seite „Analyse“ ermöglicht auf einfache Art und Weise numerische und grafische Auswertungen von Zufallsdateien. Es können alle Darstellungen auch gleichzeitig geöffnet werden. Die zu analysierende Datei wird ausgewählt:



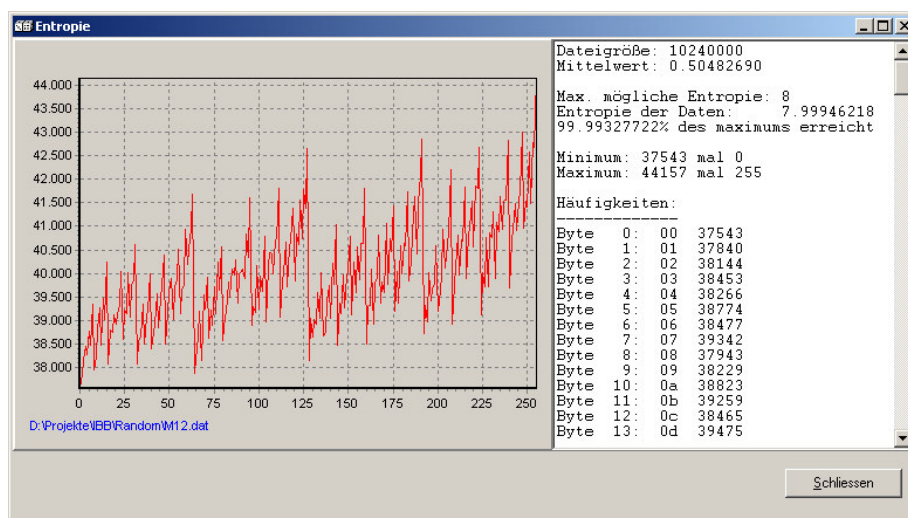
Datum: 14.08.2007		9
Dateiname: Handbuch PRG100-Software	Version: 1.4	

Entropie

Die Auswertung der Entropie (Berechnung nach Shannon) erfolgt numerisch. Graphisch werden alle Zufallsbytes in ihrer Häufigkeit dargestellt. Das folgende Beispiel zeigt gleichverteilte Zufallsdaten mit einer XOR3-Nachbearbeitung:



Das nächste Beispiel zeigt Zufallsdaten ohne digitale Nachbearbeitung. Durch die Schiefe der 0/1-Verteilung ist eine Struktur in der Grafik zu erkennen. Diese wird durch die binäre Darstellung verursacht, keinesfalls durch deterministische Anteile der Zufallsdaten.

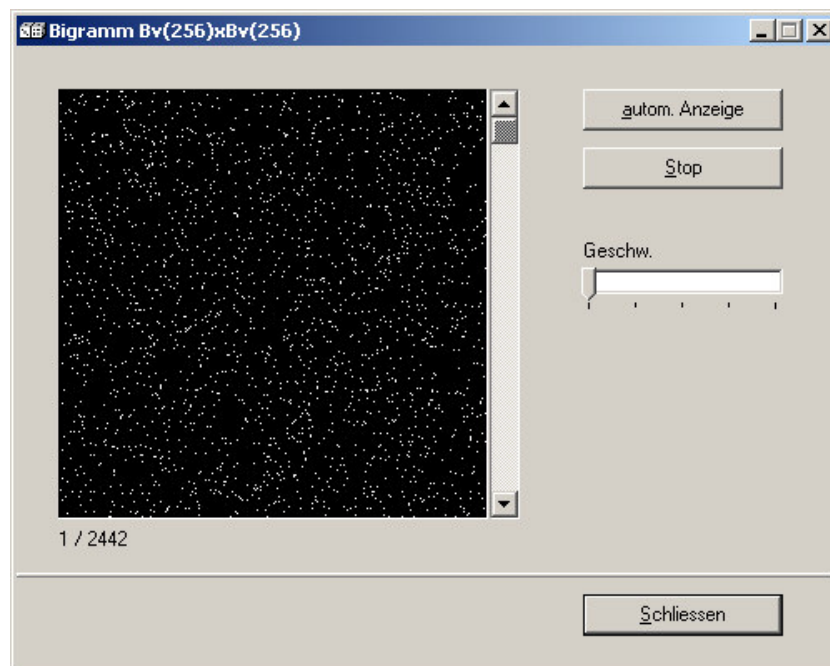


PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Bigramm-Darstellung

Bei der Bigramm-Darstellung werden zwei aufeinanderfolgende Zufallsbytes im Fenster als Punkt dargestellt. Dabei wird das erste Byte als x-Koordinate und das zweite als y-Koordinate verwendet.

Um sich die Abschnitte (eingblendet links unter dem Fenster) der Zufallsdatei komfortabel anzusehen, kann eine automatische Anzeige mit Wahl der Geschwindigkeit aktiviert und jederzeit angehalten werden.



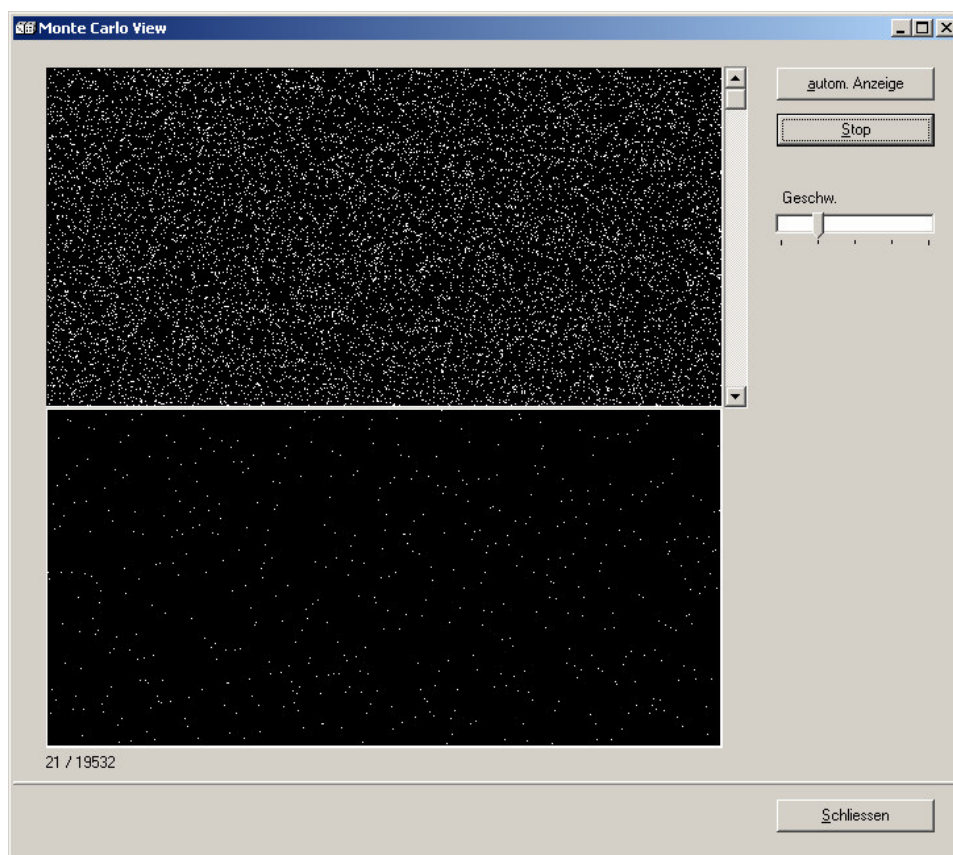
Datum: 14.08.2007		11
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Monte-Carlo-Darstellung

Bei der Monte-Carlo-Darstellung wird die x-Achse in 256 Schritte unterteilt. Im ersten Schritt der x-Achse wird der Wert des ersten Zufallsbytes in der y-Koordinate als Punkt dargestellt. Im zweiten Schritt der des zweiten Zufallsbytes. Ist der 256. Schritt als Punkt dargestellt, wird wieder mit dem ersten Schritt auf der x-Achse fortgesetzt. Das 257. Zufallsbyte wird also im ersten Schritt der x-Achse dargestellt, usw.

Das obere Fenster zeigt bereits aufaddierte Werte mehrerer Abschnitte (hier das 21. Fenster von insgesamt 19532), das untere eine aktuelle Darstellung von 256 Schritten mit ebenso vielen Zufallswerten.

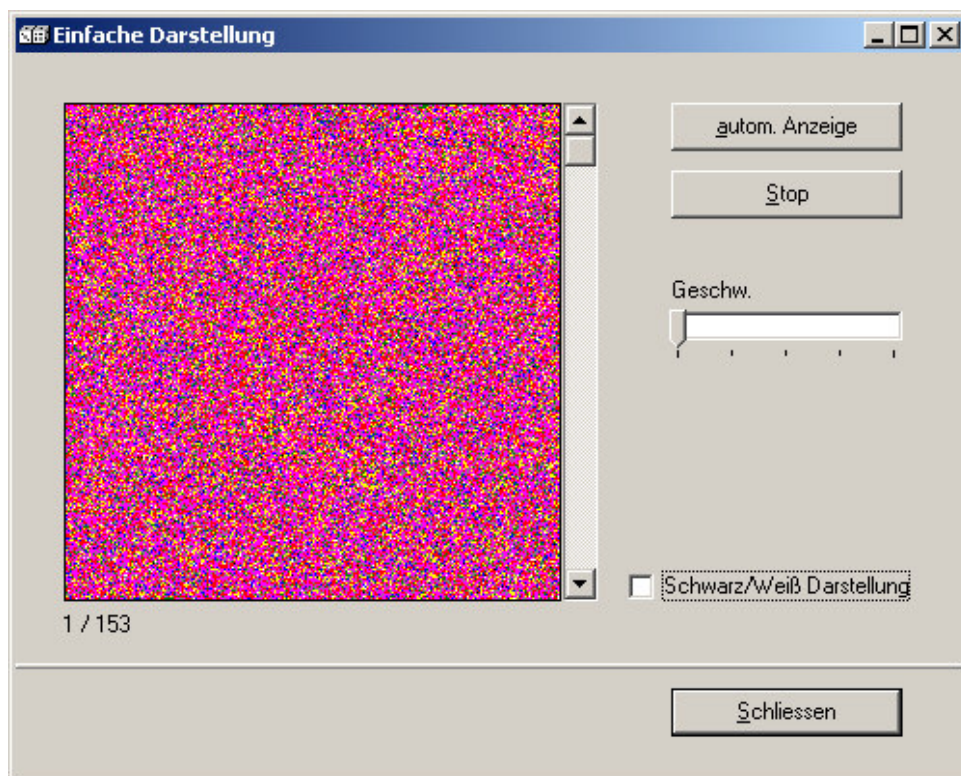


Datum: 14.08.2007		12
Dateiname: Handbuch PRG100-Software	Version: 1.4	

PRG100-Software	Handbuch	IBB Ingenieurbüro Bergmann

Einfache Darstellung

Die Zufallsdatei wird in Abschnitte unterteilt und jeweils zwei aufeinanderfolgende Zufallswerte werden in einer y-x-Koordinate als Punkt dargestellt. In der farbigen Darstellung wird jedem Zufallswert ein Farbwert zugeordnet. Beim Aktivieren der automatischen Anzeige werden je nach gewählter Geschwindigkeit alle Abschnitte der Zufallsdatei durchlaufen und angezeigt.



Datum: 14.08.2007		13
Dateiname: Handbuch PRG100-Software	Version: 1.4	