Fernschaltung über Handy mit SMS

Gunther Zielosko

1. Einleitung

Wir hatten es versprochen – im Bericht Nr. 056 „BASIC-Tiger® sendet SMS“ hatte der BASIC-Tiger® als Alarmanlage eine SMS von einem Handy an ein zweites Handy zu senden – nun werden wir diese universelle Technologie andersherum einsetzen. Wir schicken eine SMS an ein beliebig weit entferntes Handy, das diese SMS empfängt und mittels BASIC-Tiger® je nach Inhalt in verschiedene Schaltkommandos umsetzt. So können wir uns eine bezüglich Entfernung und Universalität praktisch unbegrenzte „Fernbedienung“ bauen. Stellen Sie sich als eine Anwendung beispielsweise vor, die Heizung im weit entfernten Ferienhaus lange vor Ihrer Ankunft oder bei erwartetem Frost einzuschalten. Ähnlich könnten Sie Ihr mit Standheizung ausgerüstetes Auto „vorheizen“, egal wo Sie es letzte Nacht abgestellt haben. Auch im professionellen Bereich lassen sich viele Anwendungen finden. So könnten Hotels ihre Anzeigetafeln (Zimmer frei oder belegt) am Ortseingang aktualisieren oder Wasserwirtschaftseinrichtungen ein abgelegenes Wehr ferngesteuert öffnen. Immer dann, wenn große Entfernungen eine eigenständige Draht oder Funkverbindung zum Fernschalten nicht zulassen, ist unsere einfache SMS-Fernschaltung die erste Wahl. Zudem kann der Zugriff auf die Schaltvorgänge von verschiedenen Nutzern erfolgen, Voraussetzung ist nur die Kenntnis der Nummer des „Schalthandys“ und der vereinbarte Text zum Schalten der einzelnen Verbraucher.
Im Bericht 056 haben Sie bereits viele Hinweise gefunden, wie ein Handy hardware- und softwareseitig an den BASIC-Tiger® angebunden werden kann. Wir werden uns daher im vorliegenden Bericht nicht mehr so ausführlich mit den dort beschriebenen Details beschäftigen, bei Bedarf kann man in diesem Bericht noch einmal nachschlagen. Auch hier werden wir das alte S25 von Siemens als „Versuchskaninchen“ benutzen. Das hat mehrere Gründe:

- Erstens ist es das Standard-Datenhandy schlechthin – es gibt viel Literatur, Schaltungshinweise und es hat nicht so viel „Schnickschnack“ wie viele modernen Handys.
- Zweitens ist es wahrscheinlich in großen Stückzahlen gebaut worden und liegt daher nunmehr vielfach ungenutzt im Schrank
- Drittens benutzt es der Autor immer wieder, weil er für diesen Typ jede Menge Datenkabel, lötbare Stecker usw. hat, die man beim Entwickeln braucht.

Aber auch, wenn Sie kein S25 haben, können Sie die hier vorgestellte Strategie nutzen. Einmal funktionieren auch andere Handys mit denselben oder ähnlichen Befehlen oder mit derselben Hardware. Voraussetzung für die vorgeschlagene Applikation ist jedoch, dass Ihr Handy „datenfähig“ ist und eine serielle Schnittstelle hat. Je nach Ausführung müssen Sie dann noch wissen, ob die serielle Kommunikation mit RS232- oder TTL-Pegeln erfolgt, was ggf. Ihr Datenkabel tut usw. Wenn Sie die Anschlussbedingungen Ihres seriellen Handy-Anschlusses kennen, sollten Sie fast alle Probleme lösen können.

2. Die Hardware

Prinzipiell ist alles so ähnlich wie im Bericht 056, wir werden einen simplen Economy-Tiger® verwenden, der seriell mit TTL-Pegeln arbeitet und daher nahezu direkt an das S25 angeschlossen werden kann. Die 3 Pins L80-L82 benutzen wir diesmal als Schaltausgänge, Port 6 fungiert mit den entsprechenden Steuerleitungen als Kanal für eine optionale Datenausgabe über LCD. SER1 ist im Gegensatz zum Bericht 056 die serielle Verbindung zum Handy, SER0 zeigt optional Reaktionen des Handys über ein Terminalprogramm am PC an. Voraussetzung für dieses Feature ist natürlich eine Pegelanpassung an die RS232-Signalpegel. Alles das finden Sie im Bild 1. Noch ein Hinweis – benutzen Sie bitte nicht die Hardware aus Bericht 056, hier werden die seriellen Schnittstellen andersherum verwendet!

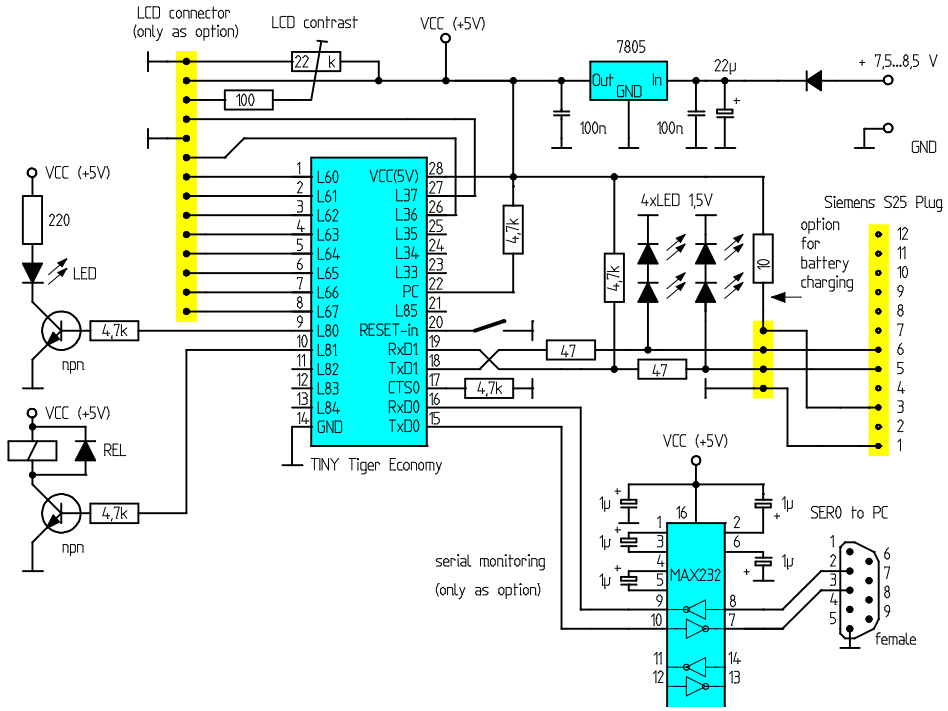

Bild 1 Die Schaltung

Sie können die Beschaltung von SER0 (MAX232, SUB-D-Buchse), LCD-Connector einschließlich der beiden Widerstände (LCD-Kontrast) sowie die als Beispiele für eine LED- bzw. Relaisstufe eingezeichneten Komponenten an L80 und L81 einfach weglassen, ohne dass die grundsätzliche Funktionalität beeinträchtigt wird. Die Schaltung und die zugehörige Software werten trotzdem Nachrichten vom Handy aus, die als SMS empfangen wurden.
Ein paar Worte zur Erklärung der einzelnen Komponenten:

TxD1: der Sendeausgang des Economy-Tigers® gibt TTL-Signale mit ca. 5V-Pegel aus (geht an Pin 6 vom Handystecker – siehe Bild 2). Das Handy dagegen arbeitet mit 3,3 V – Pegeln. Deshalb sind Maßnahmen zur Pegelbegrenzung erforderlich. Der 47 Ω - Widerstand soll mit der

Reihenschaltung der beiden LED's die Spannung (High ca. 3,3 V!) und den Strom für das Handy begrenzen.

RxD1: Das Handy sendet am Pin 5 des Steckverbinders natürlich auch nur typische 3 V – Pegel. Im Zweifelsfalle reicht das nicht, um den Economy-Tiger® richtig anzusteuern. Deshalb verwenden wir hier noch einen Pull-Up-Widerstand 4,7 kΩ an + 5 V. Zur Sicherheit wird auch hier eine Spannungsbegrenzung auf ca. 3,3 V mit zwei LED's vorgesehen.

Handy-Batterie: Pin 3 des S25-Steckers ist der Ladeeingang des Handys. Der Hersteller des S25 möchte dort eigentlich 6,1 bis 8 V bei Strömen um 1 A sehen. Wenn Sie sicherstellen können, dass die Rohspannung vor dem Regler einigermaßen stabil in diesem Bereich bleibt, können Sie Pin 3 dorthin legen. Das ermöglicht auf elegante Weise einen unbeaufsichtigten Dauerbetrieb unseres Fernschaltsystems. Vielleicht ist auch eine ausreichend leistungsfähige VCC der BASIC-Tiger®-Umgebung bei 5 V in der Lage, die Handy-Batterie nachzuladen. Da das Handy im Falle einer leeren Batterie einige 100 mA Strom zum Wiederaufladen braucht, sollte die Stromversorgung großzügig ausgelegt werden. 10 Ω dienen auch hier als „Angstwiderstand". Wenn Sie für erste Experimente auf die Wiederaufladung des Akkus verzichten wollen, lassen Sie Pin 3 des Telefon-Steckers einfach frei.

Bild 2 der Stecker des S25 und anderer Siemens-Handys

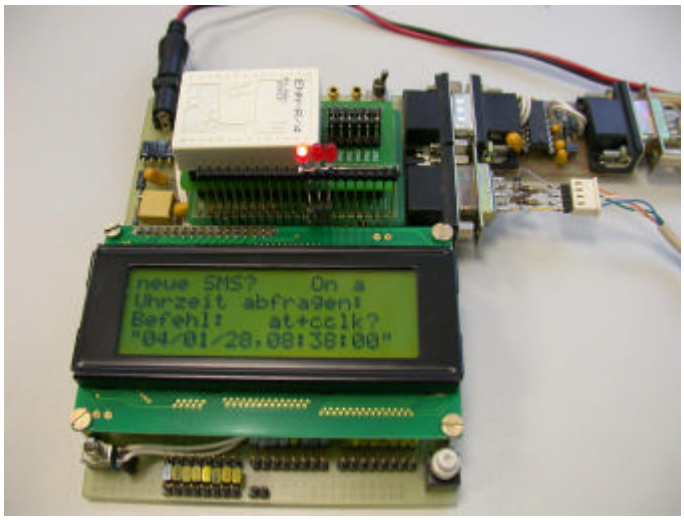

Bild 3 Versuchsaufbau des Autors

Noch ein Wort zu den Schaltausgängen. Der Economy-Tiger® liefert im ON-Zustand eines Ausganges (L80...L85) Pegel von ca. 5 V, bei OFF einen Pegel von ca. 0 V bei jeweils einigen mA Treiberfähigkeit. Für leistungsintensive Schaltaufgaben etwa am 220 V – Netz müssen geeignete Maßnahmen ergriffen werden, um Potentialtrennung (Gefahr für

Menschen), Sicherheit gegen Kurzschlüsse (Brände) und Rückwirkungen der Leistungselemente auf die Elektronik (Transienten usw.) zu gewährleisten. Solche Anwendungen sollten sich nur Fachleute auf dem Gebiet der Leistungs-Elektronik zutrauen! Eine Anregung für Nichtfachleute – verwenden Sie z.B. funkgesteuerte Fernbedienungen für Leistungs-Steckdosen aus dem Baumarkt. Der Senderteil arbeitet mit Batterien und ist galvanisch vom Stromnetz getrennt. Kleine Relais am Economy-Tiger® überbrücken die entsprechenden Taster der Fernbedienung und schalten damit spielend Netzverbraucher ein und aus. (siehe auch Bericht 026).

3. Die Auswertung einer SMS

Das Problem kennen wir bereits – eine SMS-Übertragung ist nur scheinbar das einfache Aussenden eines Textes. Im Bericht 056 mussten wir uns damit herumquälen, unseren Text in das sogenannte PDU-Format zu bringen, eher eine Strafarbeit... Aber auch beim Auslesen einer ankommenden SMS bleibt uns die Beschäftigung mit dieser kryptischen Verständigungsmethode nicht erspart, zumindest beim S25 bekommen wir wieder eine Nachricht im PDU-Format mit all ihren Bit- und Bytetransformationen. Pech gehabt – oder? Wenn man nur wenige Schaltkanäle bedienen will, wie wir in unserem Beispiel, kann man mit einem genialen Trick dieses Problem einfach umgehen. Wir wollen ja die SMS nicht wirklich lesen, sondern nur aufgrund der Meldung entscheiden, welcher Ausgang auf L und welcher auf H gelegt werden soll. Damit können wir die Auswertung erheblich vereinfachen. Folgendes Beispiel soll diese Vorgehensweise verdeutlichen:

Wir schicken die SMS zum Ein- bzw. Ausschalten eines Verbrauchers in folgender Form:

On a Verbraucher “a” an Pin L80 (im Schaltbild die LED) soll angeschaltet werden
Off b Verbraucher „b“ an Pin L81 (im Schaltbild das Relais) soll ausgeschaltet werden

Das Handy macht aus diesem einfachen Text eine unübersichtliche PDU, die neben dem eigentlichen Text noch die Ziel-Handy-Nummer, Längenangaben der Nachricht und anderes enthält. Schließlich wird dieser neue Text noch in einer umfangreichen Rechnerei von 8- auf 7-Bit-Darstellung mit anschließender Neuverteilung der Bytes umgeformt. Einzelheiten dazu finden Sie im Bericht 056 sowie dort veröffentlichten Links. Im vorliegenden Fall sieht die PDU-Darstellung etwa folgendermaßen aus:

On a wird z.B. **0001000810000044F37280C**
ist die Nummer des Zieltelefons eine andere, wird die Nachricht aber:
0001000E91946110325476980000044F37280C

Off b wird **0001000810000054FB3192406**
bzw. bei einer anderen Nummer:
0001000D91946110325476F80000054FB3192406

Schaut man aufmerksam hin, stellt man aber fest, dass die letzten Bytes unserer Nachricht jeweils identisch sind. Das heißt, wir müssen in der Regel gar nicht wissen, was in der kryptischen Nachricht alles steckt, sondern nur mit einfachen String-Befehlen den letzten Teil der PDU mit einer vorgegebenen Nachricht vergleichen, etwa so:

Wenn der rechte Teilstring der PDU = „**3192406**“ ist, soll Verbraucher **b ausgeschaltet** werden. Mit dem PC-Programm „Pduspy“, das Sie unter:

http://www.nobbi.com/download/pduspy.zip

finden oder auch mit unserem Aufbau (über SER0 und Pegelwandler) können wir uns solche Textmeldungen in PDU-Form ansehen und das Auswerteprogramm im BASIC-Tiger® entsprechend auslegen. Natürlich kann man auch den Klartext der Meldung „rückrechnen“ und damit völlig freizügig in der Wahl der Texte werden – hier soll es bei dieser einfachen Dekodierung bleiben. Testen Sie in aller Ruhe, was Ihr Handy bei vorgegebenen Textmeldungen „abliefert“ und benutzen Sie z.B. die letzten 7 Zeichen zur Verifizierung des Schaltbefehles. Wichtig ist auch die genaue Schreibweise, so bringt z.B. ein (unsichtbares!) Leerzeichen beim Eintippen am Handy den PDU-String durcheinander. Ähnliches passiert auch manchmal bei SMS-Meldungen, die über Internet oder andere Nicht-Telefon-Verbindungen zustande kommen, z.B. hängt noch Werbung dran oder ähnliches. Unser einfacher „Entschlüsselungsmechanismus“ wäre in so einem Fall überfordert. Wenn nötig, muss man dann die auf dem Handy ankommende und auf SER0 in PDU-Form angezeigte Meldung als (vielleicht alternativen) Vergleichsstring benutzen.

4. Das Programm HANDY_02.TIG

Der Rest ist einfach. Analog zum Programm „HANDY_01.TIG“ aus dem Bericht 056 werden auch hier am Anfang ein paar AT-Befehle an das Handy geschickt und Reaktionen abgefragt. Wenn Ihr Aufbau also fertig ist und Sie ein S25 angeschlossen haben, starten Sie nun das hier mitgelieferte Programm „HANDY_02.TIG“. Wenn Sie außer dem Handy nichts weiter angeschlossen haben (also kein Display, keinen RS232-Pegelwandler), sollte Ihr S25 jetzt wenigstens kurz klingeln – ein Zeichen dafür, dass die Kommunikation klappt. Da insbesondere der Klingelbefehl AT^SRTC siemensspezifisch ist, kann das bei anderen Handys ins Leere gehen. Wenn es bei Ihrem Telefon ein anderes Kommando zum Klingeln gibt, sollten Sie den Befehl im Programm anpassen. Bei angeschlossenem Display und/oder Terminalprogramm an SER0 können Sie alle gesendeten bzw. empfangenen Daten beobachten. Danach geht das Programm in eine „endlose“ Schleife und fragt beim Handy ca. alle 15 Sekunden nach, ob eine neue (bisher ungelesene) SMS eingegangen ist. Dazu dient der AT-Befehl AT+SMGL=1. Die Reaktion des Handys ist entweder OK oder die PDU-Form der Nachricht. Wenn das der Fall ist, wird diese von allen unwesentlichen Zeichen (z.B. Zeilenwechsel, „OK“ usw.) befreit, ihr Inhalt getestet und entsprechende Schaltvorgänge ausgelöst. Damit der entsprechende Handyspeicher nicht „überläuft“, werden mit den Befehlen AT+CMGD=1 bis AT+CMGD=4 alle (?) gespeicherten SMS gelöscht. Mit einem Terminal-Programm (und einem Pegelwandler!) können Sie das Frage- und Antwortspiel auf

SER0 mit 19200 Baud auf einfache Weise protokollieren (Bild 3). Sie werden feststellen, dass in unserem Demo-Programm bei jeder Abfrage zusätzlich Datum und Uhrzeit mit abgefragt und übertragen werden. Ein toller Zusatzdienst für eventuelle Recherchen und weitere Aufgabenstellungen.

```
Uhrzeit abfragen:
at+cclk?
+cclk: "04/01/28,08:20:00"

OK

at+cmgl=0
+CMGL: 3,0,,24
07919471016700002400D91946190039184F900004010828012204004 4F37280C

OK
```

Bild 3 Auszug aus dem seriellen Protokoll des Programms

Das vorliegende Demoprogramm HANDY_02.TIG „kennt“ bisher nur die folgenden Befehle:

On a	Off a	Schaltet L80 auf high bzw. low
On b	Off b	Schaltet L81 auf high bzw. low
On c	Off c	Schaltet L82 auf high bzw. low
	Off all	Schaltet L80, L81 und L82 auf low

Andere Meldungen werden ignoriert und führen nicht zu Schalthandlungen, auch wenn der fragliche Text in ihnen enthalten sein sollte.

Wenn Sie vertraut mit den AT-Befehlen sind, werden Ihnen weitere Möglichkeiten einfallen (Sender der SMS identifizieren, Ladezustand kontrollieren, Messwerte übertragen usw.) Denken Sie bei allen Anwendungen auch daran, dass eine SMS nicht immer sofort den Empfänger erreicht, z.B. wenn das Netz überlastet ist usw. Zeitkritische Applikationen lassen sich auf diesem Wege nur sehr schwer realisieren! Trotzdem ist das Schalten über SMS eine reizvolle Bereicherung für Hobbyelektroniker. Berücksichtigt man, dass der reine Empfangsbetrieb des Handys nichts kostet, kann man sich einen teuren Vertrag für das „Schalthandy“ sparen. Vorteilhaft ist hier ein abgelegtes Handy und ein möglichst billiger Vertrag z.B. mit Prepaid-Karte. Damit fallen für das Empfänger-Handy außer dem (einmaligen) Handyvertrag keine weiteren Kosten mehr an. Auf der Senderseite kann man entweder ein anderes Handy benutzen oder mit etwas Glück einen kostenlosen bzw. wenigstens preiswerten SMS-Dienst finden – damit sind die Kosten für diese „weltweite Fernbedienung“ dann wirklich vernachlässigbar.

5. Fehlersuche und weitere Experimente

Spätestens dann, wenn etwas nicht funktioniert, brauchen wir ein wenig Handwerkszeug, um die Kommunikation mit einem Handy zu untersuchen. Mindestvoraussetzung ist ein

(serielles) Datenkabel, das zu unserem Handy passt. Dieses Kabel enthält mehr als nur ein paar Drähte - wir wissen, dass das Gerät nur TTL-Pegel (sogar nur 3 V) benutzt, die serielle Schnittstelle des PC aber RS232-Pegel (also –3...-15 V und +3...+15V). Im Kabel muß sich also ein Pegelwandler befinden, der aus unbenutzten Signalleitungen der RS232-Schnittstelle des PC mitversorgt wird. Stecken wir ein solches Kabel in das Telefon und in den PC, sollte bereits ein Datenaustausch möglich sein. Software zum Kommunizieren hat eigentlich jeder Windows-PC dabei, früher (z.B. unter Windows 3.1.) hieß das Programm „Terminal“, jetzt finden Sie unter Zubehör und Kommunikation oft ein Programm namens „Hyper-Terminal“. Da dieses aber deutlich komplizierter ist als das alte, hat der Autor die einfachere Version „Terminal“ diesem Bericht beigelegt, es sollte auch unter Windows 98, 2000, ME und XP funktionieren. Mit diesem Programm können nahezu alle Kommunikationstests durchgeführt werden, die wir benötigen. Starten wir also dieses Programm (es ist eine einfache Exe, die nicht installiert werden muß, und nehmen wir ein paar Einstellungen vor:

Unter Einstellungen und Datenübertragung bzw. Terminal-Einstellungen richten wir folgendes ein:

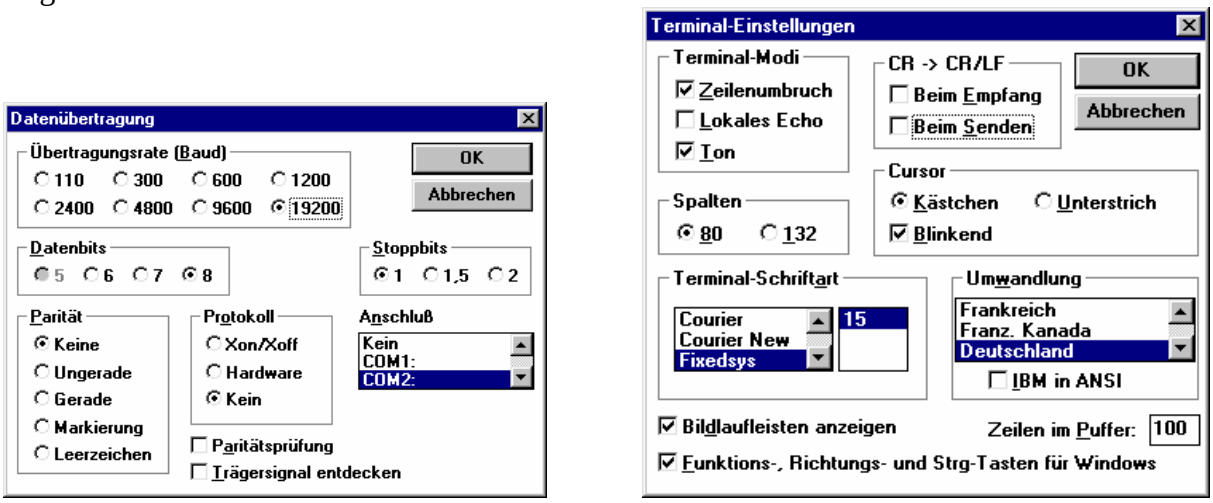

Bild 4 Einstellungen im Programm Terminal.exe

Die Schnittstelle können Sie natürlich je nach Ihrem PC selbst auswählen. Als letztes wird unter Einstellungen, Terminalemulation die Einstellung TTY (allgemein) vorgenommen.

Jetzt erhalten Sie eine freie Schreibfläche, in die Sie einen ersten Befehl eintragen können, etwa so (egal, ob groß – oder kleingeschrieben):

at+cclk? (und danach ENTER)

bei etwas Glück erscheint direkt unterhalb der eingegebenen Zeile die Antwort des Telefons:

cclk: 04/01/28, 08:20:00 (das aktuelle Datum und die Uhrzeit)

Mit dem Terminalprogramm und Ihrem angeschlossenen Handy können Sie sich nun durch die Welt der AT-Befehle bewegen. Probieren Sie aber möglichst nur Befehle aus, die Ihr S25 nicht dramatisch verändern, da gibt es nämlich einige! Lesen Sie zunächst die Liste der für das S25 gültigen Befehle und ihre Folgen gründlich durch, bevor Sie loslegen! Wichtig ist auch, dass Sie nach jedem Befehl erst die Reaktion Ihres S25 abwarten sollten, bevor Sie einen neuen starten.
Dann aber können Sie sich mit diesen Kenntnissen, Ihrem Aufbau mit dem Economy-Tiger® und mit Tiger-BASIC® an ganz neue Aufgaben heranwagen. Alles, was Sie mit dem Terminalprogramm am Handy anstellen können, lässt sich auch vom BASIC-Tiger® aus durchführen. Andere Handys sind dann ebenfalls kein unlösbares Problem mehr...

Für diejenigen, die sich das Medium SMS für den BASIC-Tiger® nun weiter erschließen wollen, hat Wilke Technology zeitgleich einen Modulsatz zum Chiffrieren und Dechiffrieren von Meldungen im PDU-Mode bereitgestellt. Er besteht aus drei Dateien, der Include-Datei sms_v004.inc und den beiden Tiger-Programmen sendSMS.TIG und receiveSMS.TIG, die diesem Bericht ebenfalls beiliegen. Hiermit eröffnen sich für den Anwender weitere Möglichkeiten zur Nutzung der SMS-Technologie. Die erforderliche Softwareentwicklung auf der Anwenderseite wird dadurch erheblich verringert.

Viel Spaß mit Ihrem neuen Spielzeug!