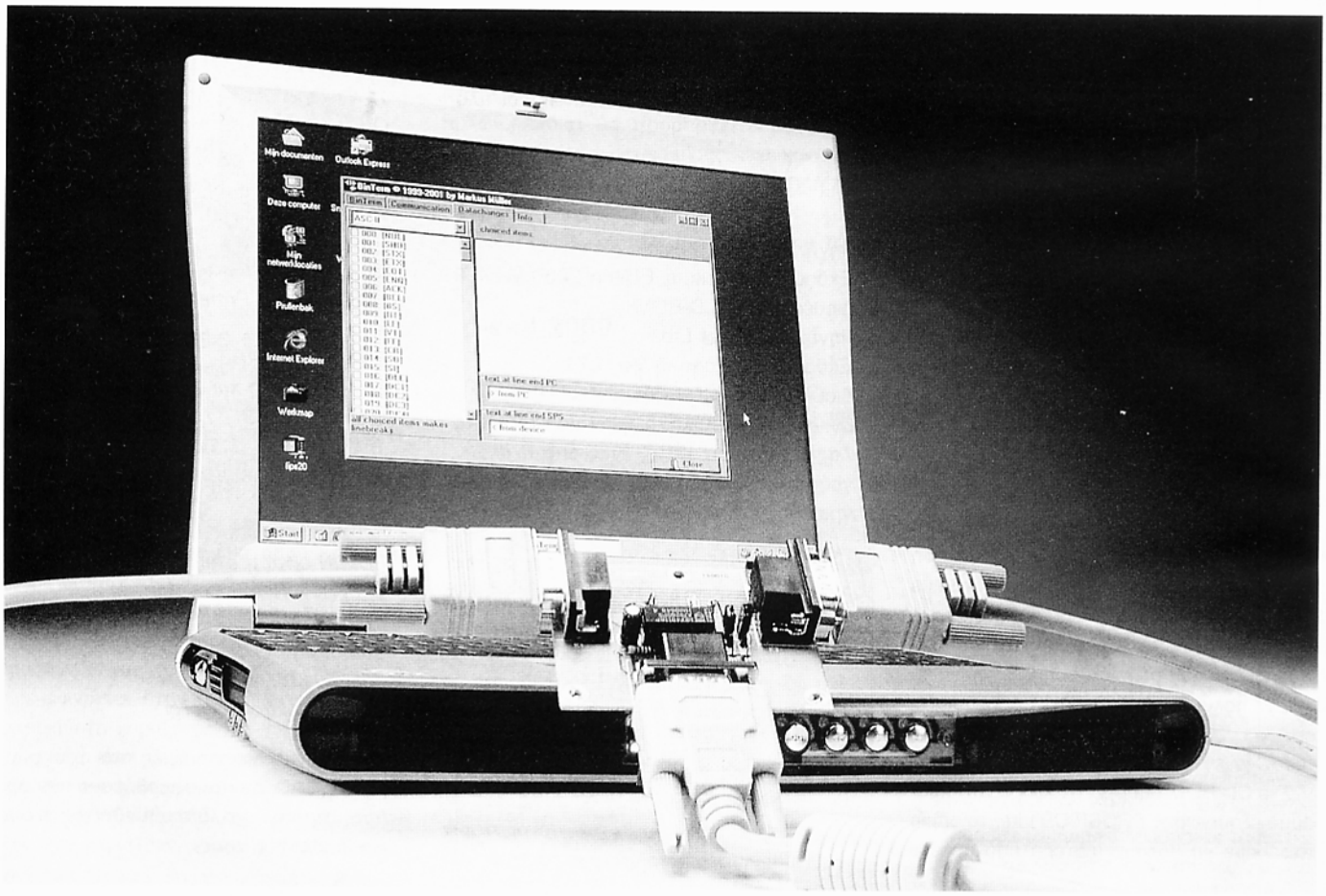
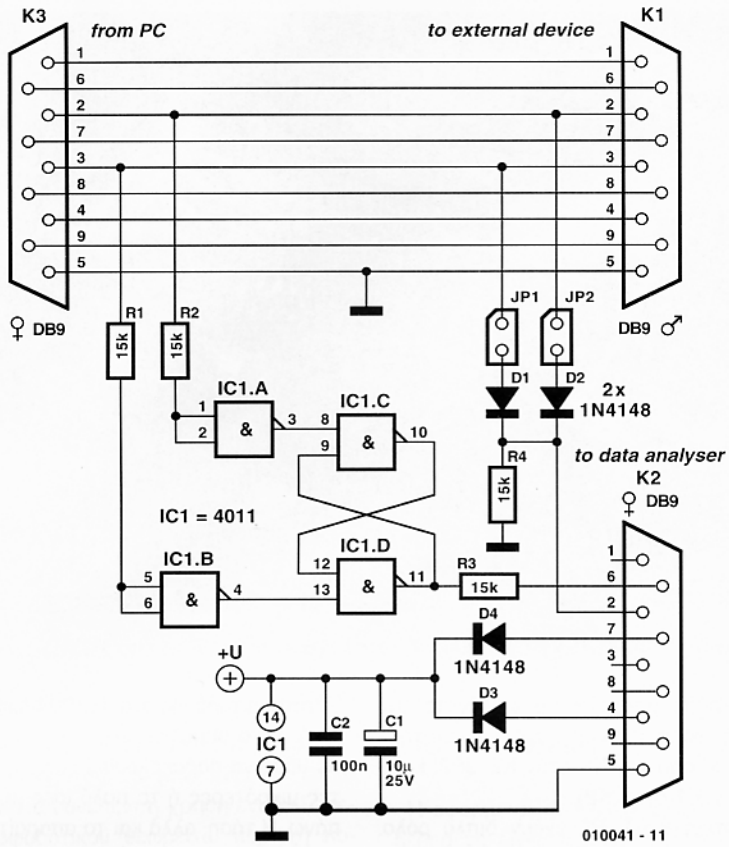
Ένας κατάσκοπος στη σειριακή θύρα

άμεση ανάλυση των διακινούμενων δεδομένων

Μια μικρή πλακέτα, τοποθετημένη σε σειρά με το καλώδιο σειριακής σύνδεσης δύο συσκευών αρκεί για να παρακολουθεί και να καταγράφει την κίνηση μιας ζεύξης RS232. Οι τιμές των διακινούμενων byte απεικονίζονται στην οθόνη ενός συνηθισμένου PC μέσω του κατάλληλου λογισμικού.

Είναι βέβαιο πως και μόνο η λέξη 'κατάσκοπος' φέρνει στο μυαλό μας την εποχή του ψυχρού πολέμου, ή στους πιο νέους από εμάς, κινηματογραφικές ταινίες με τον James Bond. Ευτυχώς ή δυστυχώς όμως, το κύκλωμά μας δεν έχει σχέση με τίποτα από αυτά. Θα λέγαμε ότι είναι πολύ πιο 'νόμιμο' από ότι φανταζόμαστε αφού η κύρια χρήση του αφορά στην ανίχνευση και αντιμετώπιση σφαλμάτων σχετικών με τις σειριακές μεταδόσεις. Η αξία της είναι αναμφισβήτητη αφού οι περισσότερες περιφερειακές συσκευές επικοινωνούν με τον υπολογιστή που τις ελέγχει, μέσω ζεύξεων αυτού του τύπου. Άλλωστε, το ίδιο εύκολα μπορούν να 'μιλήσουν' και δύο υπολογιστές μεταξύ τους, ανταλλάσσοντας δεδομένα. Εκτός από τα παραπάνω δεν πρέπει να παραλείψουμε τη χρήση του 'κατασκόπου' για εκπαι-





Σχ. 1. Το υλικό μέρος της κατασκευής είναι πολύ 'λιτό'. Για την τροφοδοσία φροντίζει ο υπολογιστής στον οποίο συνδέεται η κατασκευή.

δευτικούς σκοπούς. Με τη βοήθειά του οι σπουδαστές είναι σε θέση να ανακαλύψουν τα μυστικά των πρωτοκόλλων σειριακής επικοινωνίας επινοώντας, ίσως, κάποια καινούργια.

Το κύκλωμα της κατασκευής εισάγεται μεταξύ δύο σειριακών συσκευών. Για τον σκοπό αυτό είναι εφοδιασμένο με δύο συνδετήρες μέσω των οποίων παρεμβάλλεται στους αγωγούς της ζεύξης. Ένας ακόμα είναι απαραίτητος για την μεταφορά των byte που 'συλλαμβάνει' σε έναν PC. Ο τελευταίος είναι εκείνος που 'τρέχοντας' το κατάλληλο λογισμικό δείχνει στην οθόνη του τις τιμές των διακινούμενων byte. Η χρήση της κατασκευής είναι πολύ απλή.

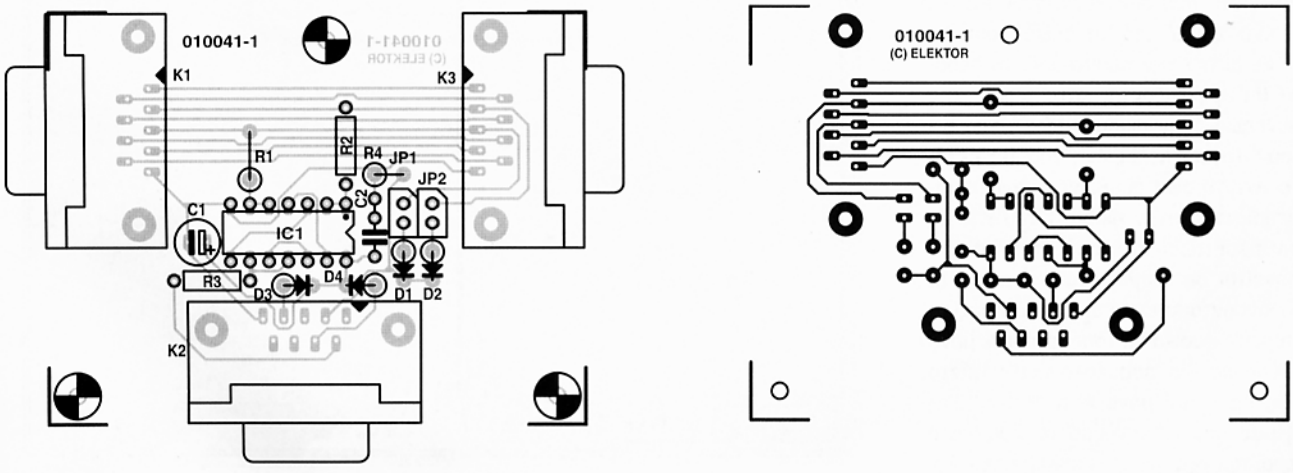
Όλες οι απαραίτητες ρυθμίσεις και επιλογές πραγματοποιούνται μέσω του λογισμικού που είναι γραμμένο στη γλώσσα Delphi της Borland και είναι συμβατό με τα λειτουργικά Windows 9x και NT. Οι τιμές των διακινούμενων byte απεικονίζονται σε μορφή ASCII, δεκαδική ή δεκαεξαδική. Η ίδια η συσκευή είναι σε θέση να καταγράψει και να εμφανίσει την κίνηση και στις δύο γραμμές της σειριακής ζεύξης (RxD, TxD) με την προϋπόθεση ότι οι δύο συρμοί των δεδομένων δεν μεταδίδονται ταυτόχρονα (ημιαμφίδρομη μετάδοση). Αν τοποθετήσετε δύο ίδιες σε σειρά μπορείτε να παρακολουθείτε την κίνηση ακόμα και αν η ανταλλαγή των δεδομένων στις δύο γραμμές πραγματοποιείται ταυτόχρονα (αμφίδρομη μετάδοση). Ένας περιορισμός λέει ότι η ταχύτητα μετάδοσης στις δύο γραμμές πρέπει να είναι η ίδια. Σε ότι αφορά στην

Κατάλογος εξαρτημάτων

Αντιστάσεις:
R1-R4 = 15KΩ

Πυκνωτές:
C1 = 10μF 25V κατακόρυφος
C2 = 100nF
Ημιαγωγοί:
D1-D4 = 1N4148
IC1 = 4011

Διάφορα:
K1 = συνδετήρας sub D 9 ακίδων (αρσενικός) για τυπωμένο κύκλωμα
K2,K3 = συνδετήρας sub D 9 επαφών (θηλυκός) για τυπωμένο κύκλωμα
JP1,JP2 = βραχυκυκλωτήρες
Τυπωμένο κύκλωμα, κωδικός: 010041-1
Λογισμικό, κωδικός: 010041-11 (διατίθεται δωρεάν από το Δικτυακό τόπο του Ελέκτορ)



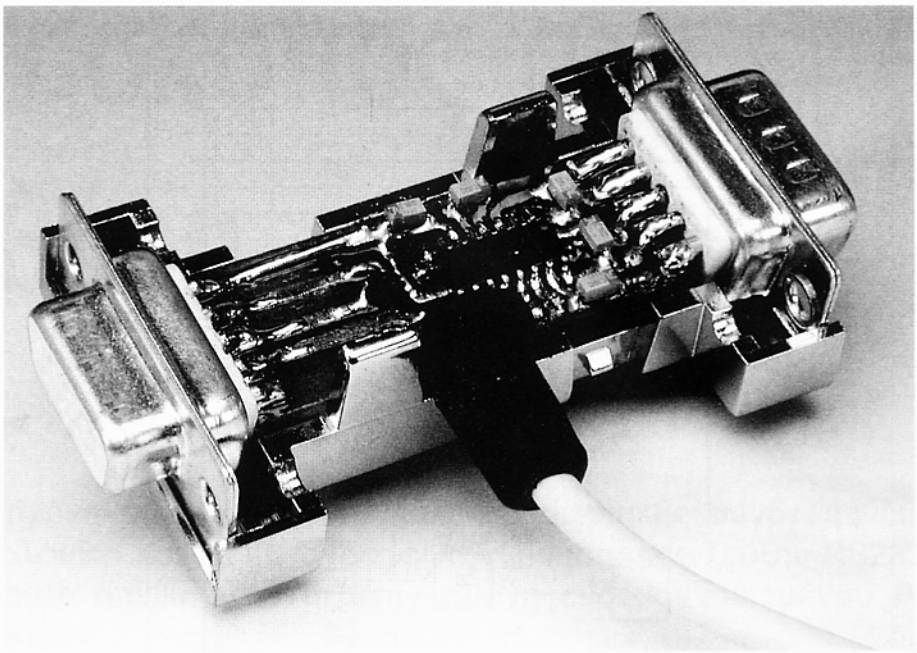
Σχ. 2. Το τυπωμένο κύκλωμα και η τοποθέτηση των υλικών στην πλακέτα.

τροφοδοσία, ο 'κατάσκοπος' είναι εξαιρετικά φειδωλός. 'Δανείζεται' την απαραίτητη ισχύ λειτουργίας από τη σειριακή θύρα του υπολογιστή στον οποίο αναμεταδίδει τα διακινούμενα δεδομένα.

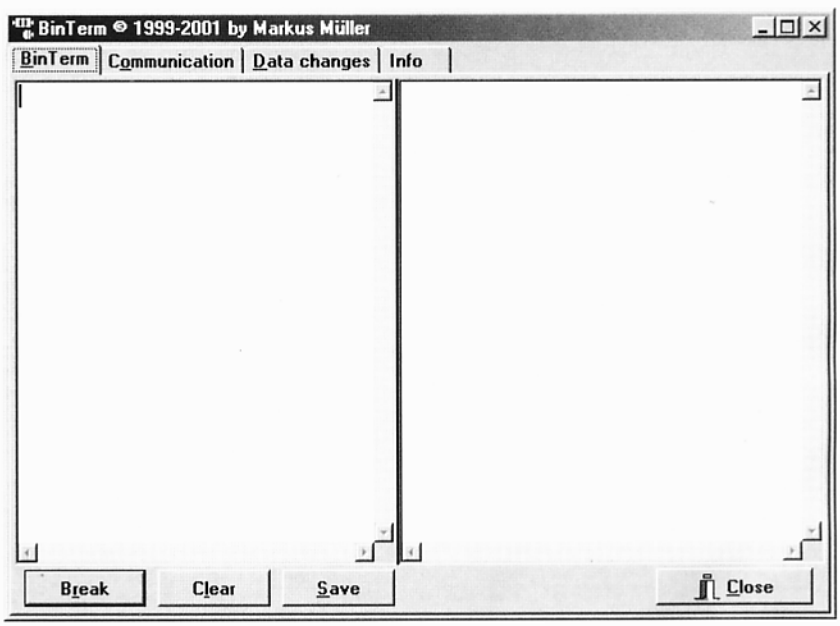
Το υλικό

Μια σύντομη ματιά στο διάγραμμα του σχ. 1 πείθει πως το κύκλωμα της κατασκευής είναι εξαιρετικά απλό. Εκτός από το (μοναδικό) ολοκληρωμένο και τους τρεις συνδετήρες αρκείται σε δέκα μόνο παθητικά εξαρτήματα.

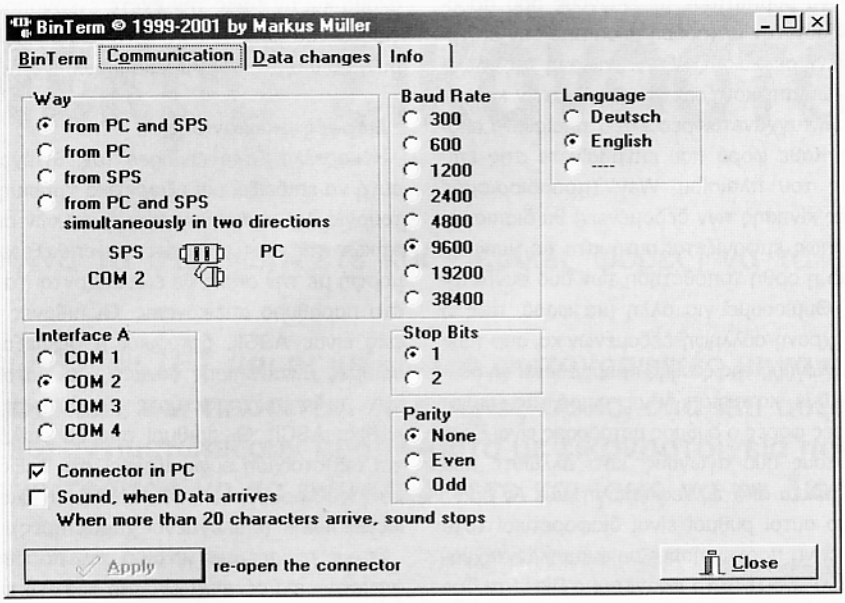
Οι συνδετήρες K1 και K3 είναι εκείνοι μέσω των οποίων διέρχονται οι σειριακοί συρμοί των δεδομένων. Όπως εύκολα γίνεται αντιληπτό, όλες οι ακίδες του ενός συνδέονται μια προς μια με τις ακίδες του δεύτερου χωρίς τη μεσολάβηση κανενός εξαρτήματος. Μια περισσότερο προσεκτική ματιά μας οδηγεί στο συμπέρασμα πως μόνο οι γραμμές TxD και RxD αξιοποιούνται από την κατασκευή. Η πρώτη από αυτές δραστηριοποιείται όταν γίνεται μετάδοση από τα αριστερά προς τα δεξιά, ενώ η δεύτερη όταν η μετάδοση έχει την αντίθετη φορά. Οι παλμοί που εμφανίζονται σε αυτές αναστρέφονται από τις πύλες A και B του IC1, για να οδηγηθούν στη συνέχεια στις εισόδους Τοποθέτησης (Set) και Επανατοποθέτησης (Reset) του φλιπ – φλοπ SR που σχηματίζουν οι υπόλοιπες πύλες του ίδιου εξαρτήματος. Η έξοδος του φλιπ – φλοπ οδηγείται στην ακίδα DSR του K3 για να ενημερώσει τον υπολογιστή που παρακολουθεί την ζεύξη για την φορά κίνησης των δεδομένων. Οι δίοδοι D1, D2 μαζί με την R4 σχηματίζουν μια πύλη Ή στην οποία καταλήγουν οι παλμοί των γραμμών RxD και TxD. Έτσι αν για παράδειγμα έχουν τοποθετηθεί και οι δύο, και υπάρχει δραστηριότητα στην ακίδα 2 του K1, τότε η ακίδα 11 του φλιπ – φλοπ θα οδηγηθεί σε χαμηλή στάθμη υποδηλώνοντας στον υπολογιστή που συνδέεται στον K3 ότι η κίνηση έχει φορά από τα δεξιά προς τα αριστερά. Σε αυτήν την περίπτωση, τα δεδομένα που θα εμφανίζονται κατά μήκος της R4 και συνεπώς στην ακίδα 2 (TxD) του K3 θα αφορούν στη συγκεκριμένη γραμμή μετάδοσης. Το αντίστροφο συμβαίνει όταν υπάρχει δραστηριότητα στην ακίδα 3 του K3. Σε αυτήν την περίπτωση η έξοδος του φλιπ – φλοπ οδηγείται σε υψηλή στάθμη, αφού τα δεδομένα κινούνται από τα αριστερά προς τα δεξιά. Μπορείτε φυσικά να τοποθετήσετε μόνο τη μια δίοδο και να παρακολουθείτε πάντα την κίνηση προς μια μόνο κατεύθυνση. Στη σχεδίαση μας, για να κάνουμε τα πράγματα ευκολότερα, προτιμήσαμε να κολλήσουμε και τις δύο διόδους τοποθετώντας σε σειρά με αυτές ισάριθμους βραχυκυκλωτήρες. Με αυτόν τον τρόπο μπορείτε να επιλέγετε την επιθυμητή φορά κίνησης χωρίς κολλητήρι. (JP1: κίνηση από τον K3 στον K2, JP2: κίνηση από τον K1 στον K2).



Οι αντιστάσεις R1, R2 έχουν διπλό ρόλο. Από τη μια πλευρά προστατεύουν τις εισόδους των δύο πυλών από υπερτάσεις, ενώ από την άλλη, σε συνεργασία με τις εσωτερικές δίοδους των δύο πυλών, προστατεύουν το ολοκληρωμένο από τις αρνητικές τάσεις που εμφανίζονται στις γραμμές RS232. Οι τιμές τους είναι τέτοιες ώστε σε συνδυασμό με τις εσωτερικές χωρητικότητες των εισόδων του IC1 να περιορίζουν την μέγιστη ταχύτητα μετάδοσης στα 38400 baud (38,4 kbit/sec). Αυτό σημαίνει πως ο 'κατάσκοπος' είναι σε θέση να παρακολουθεί ζεύξεις με ταχύτητες μικρότερες ή το πολύ ίσες με την παραπάνω. Η τάση, αλλά και το απαραίτητο ρεύμα, τροφοδοσίας της κατασκευής παρέχονται από τον συνδετήρα K2 ή ορθότερα από τον υπολογιστή που παίζει τον ρόλο του επόπτη. Το λογισμικό φροντίζει να οδηγεί τις ακίδες 4 (DTR) και 7 (RTS) του συνδετήρα K2 σε υψηλή στάθμη, η οποία, μέσω των διόδων D3 και D4, φθάνει στην ακίδα 14 του IC1. Η τάση φιλτράρεται μέσω του C1 και ο θόρυβος καταστέλλεται από τον C2. Οι απαιτήσεις σε



Σχ. 3. Το βασικό παράθυρο που ανοίγει μόλις 'τρέξουμε' το BinTerm. Κάθε ένα τμήμα του παραθύρου αφορά σε μια από τις δύο ροές δεδομένων.



Σχ. 4. Η καρτέλα 'Communications' επιτρέπει τη ρύθμιση των παραμέτρων επικοινωνίας.

ρεύμα είναι σχεδόν μηδενικές, με αποτέλεσμα ο υπολογιστής να μην 'νοιώθει' καμία φόρτιση. Κατά συνέπεια η χρήση ενός εξωτερικού τροφοδοτικού θεωρείται περιττή πολυτέλεια.

Στο σχ. 2 φαίνεται η πλακέτα και η τοποθέτηση των υλικών πάνω σε αυτήν. Η συναρμολόγηση της δεν θα απαιτήσει περισσότερο από μια ώρα. Τα εξαρτήματα είναι λιγοστά με αποτέλεσμα, αν είστε επαρκώς προσεκτικοί, να έχετε μια κατασκευή που θα 'δουλέψει με την πρώτη'.

Το λογισμικό

Η εφαρμογή που διαχειρίζεται τα σειριακά δεδομένα είναι γραμμένη σε γλώσσα Delphi 5. Ονομάζεται BinTerm από τις λέξεις Binary Terminal (Δυαδικό Τερματικό). Μπορείτε να την 'κατεβάσετε' δωρεάν από την ιστοσελίδα του Ελέκτορ, αναζητώντας την με τον κωδικό 010041-11. 'Τρέχει' κάτω από το περιβάλλον των Windows 9x και NT, χωρίς να απαιτεί εγκατάσταση (αποτελείται μόνο από το πρόγραμμα binterm.exe). Κάθε φορά που τερματίζεται, όλες οι ρυθμίσεις και οι παράμετροι που έχετε ορίσει αποθηκεύονται σε ένα αρχείο τύπου .INI.

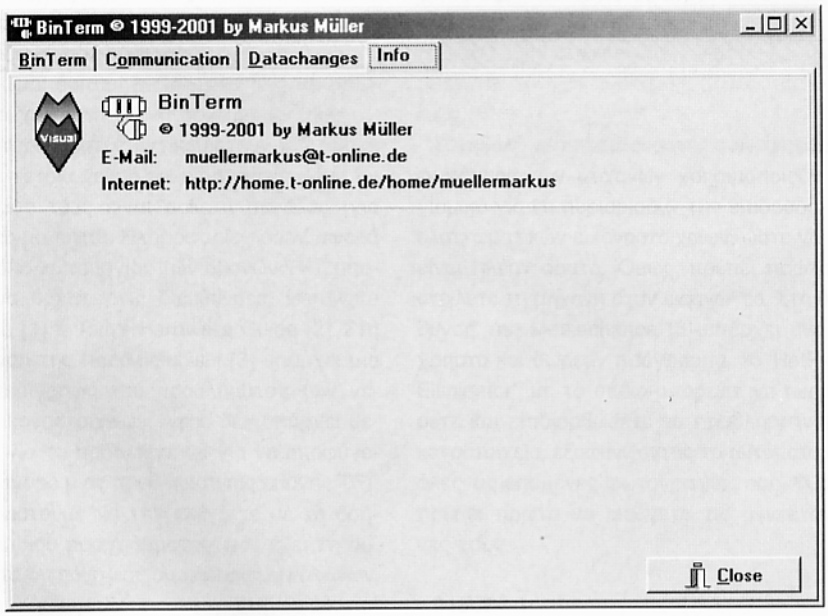
Το πρόγραμμα έχει κάτω από την εποπτεία του τρεις διαφορετικές λειτουργίες:

Κύρια λειτουργία: διαχείριση όλων των εικονικών ρυθμιστικών

Λειτουργία ανάγνωσης σειριακής θύρας: αποθηκεύει όλα τα εισερχόμενα byte (χαρακτήρες) σε μια κυκλική μνήμη 94000 θέσεων

Λειτουργία απεικόνισης: 'διαβάζει' τα byte από τη μνήμη και τα απεικονίζει στην οθόνη.

Οι λειτουργίες αυτές εκτελούνται ανεξάρτητα η μια από την άλλη, αλλά όχι ταυτόχρονα. Κάτι τέτοιο δεν είναι επιτρεπτό από το περιβάλλον των Windows. Για να μειωθούν οι συνέπειες αυτής της αδυναμίας, έχουν οριστεί προτεραιότητες στην εκτέλεσή τους. Η ανάγνωση της σειριακής θύρας έχει την μέγιστη προτεραιότητα, η απεικόνιση διατηρεί την δεύτερη, ενώ η διαχείριση των εικονικών ρυθμιστικών την τρίτη. Σύμφωνα με αυτήν την τακτική, η συλλογή και καταγραφή των byte πραγματοποιείται με τη μέγιστη δυνατή ταχύτητα για να ακολουθήσει λίγο αργότερα η απεικόνισή τους. Στην περίπτωση που η ροή των εισερχόμενων byte είναι εξαιρετικά μεγάλη, ή ο 'νεκρός' χρόνος που μεσολαβεί κάθε φορά που αλλάζει η φορά κίνησης των δεδομένων είναι πολύ μικρός, τότε είναι πολύ πιθανό ο υπολογιστής να μην προφταίνει να 'ξεκαθαρίζει' εγκαίρως την φορά κίνησης. Σε μια τέτοια περίπτωση τα πρώτα byte της νέας φοράς κίνησης θα εμφανίζονται σαν τελευταία της προηγούμενης.



Σχ. 5. Μέσα από την καρτέλα 'Data changes' μπορείτε να επιλέξετε έναν από τρεις διαφορετικούς τρόπους απεικόνισης των εισερχόμενων byte.

Χρήση

Λίγο δευτερόλεπτα μετά την εκκίνηση του BinTern.exe θα δείτε στην οθόνη του υπολογιστή σας ένα λευκό παράθυρο συνοδευόμενο από τα εικονικά πλήκτρα της εφαρμογής. Μέσα σε αυτό απεικονίζονται οι τιμές των byte που διακινούνται στην εποπτευόμενη ζεύξη. Στην περίπτωση που έχετε συνδέσει δύο 'κατασκόπους' σε σειρά, προκειμένου να παρακολουθείτε την κίνηση προς τις δύο κατευθύνσεις ταυτόχρονα, τότε η οθόνη χωρίζεται σε δύο παράθυρα. Ένα για κάθε φορά κίνησης των δεδομένων. Το διπλό παράθυρο φαίνεται στο σχ. 3. Η σημασία των εικονικών πλήκτρων είναι η εξής:

Break: διακόπτει προσωρινά την απεικόνιση των δεδομένων

Clear: διαγράφει τα περιεχόμενα του παραθύρου απεικόνισης

Save: αποθηκεύει τα απεικονιζόμενα δεδο-

μένα σε ένα αρχείο κειμένου

Close: τερματίζει την εφαρμογή

Στην περίπτωση που το ζητούμενο είναι η εξαγωγή από το παράθυρο απεικόνισης ενός συγκεκριμένου πλήθους χαρακτήρων ή γραμμών, ο χρήστης έχει στη διάθεση του τις λειτουργίες της Αντιγραφής (Control-c) και της επικόλλησης (Control-v) που υποστηρίζονται εγγενώς από τα Windows. Αμέσως μετά το πρώτο κλικ στο πλήκτρο Break, το όνομά του αλλάζει σε Continue. Με το δεύτερο αποκτά το αρχικό του όνομα ενώ η απεικόνιση που είχε διακοπεί, ξαναρχίζει. Στην περίπτωση που το BinTerm έχει ανοίξει και τα δύο παράθυρα απεικόνισης, τότε το περιεχόμενο του αριστερού αποθηκεύεται στο αρχείο κειμένου κάτω από τον τίτλο 'Left Box' (Αριστερό πλαίσιο κειμένου), ενώ το περιεχόμενο του δεξιού κάτω από τον τίτλο 'Right Box' (Δεξιό πλαίσιο κειμένου).

Επικοινωνίες

Κάνοντας κλικ στην καρτέλα Communication, εμφανίζεται μια καινούργια, που κύριο έργο της είναι ο προκαθορισμός των παραμέτρων επικοινωνίας (σχ. 4). Στη συνέχεια θα επιχειρήσουμε μια σύντομη εξήγηση των όσων απεικονίζονται.

Το πλήκτρο 'Apply' προκαλεί την επανεκκίνηση του προγράμματος λαμβάνοντας υπ' όψη τις παραμέτρους που έχουν δηλωθεί. Το πλήκτρο 'Close' τερματίζει το πρόγραμμα.

Το πλαίσιο Baud Rate χρησιμοποιείται για τον ορισμό της ταχύτητας και των λοιπών παραμέτρων (μήκος λέξης, ψηφία λήξης και ισοτιμίας) που αφορούν στην μετάδοση των δεδομένων. Οι αριθμοί που θα δηλωθούν οφείλουν να συμπίπτουν με εκείνους που προσδιορίζουν την μετάδοση μέσα από την επιτηρούμενη σειριακή ζεύξη. Η επιλογή της γλώσσας των απεικονιζόμενων μηνυμάτων και μενού επιτυγχάνεται μέσω του πλαισίου Language. Κάθε φορά που επεμβαίνετε στις επιλογές του πλαισίου 'Way' (προσδιορισμός φοράς κίνησης των δεδομένων) θα διαπιστώνετε πως εμφανίζεται αυτόματα με γραφικό τρόπο η ορθή τοποθέτηση των δύο συνδετήρων. Θυμίσουμε για άλλη μια φορά, πως η ταυτόχρονη 'σύλληψη' δεδομένων και από τους δύο αγωγούς της ζεύξης προϋποθέτει τη σύνδεση δύο 'κατασκόπων' σε σειρά. Τις περισσότερες φορές ο ρυθμός μετάδοσης είναι ίδιος και στους δύο αγωγούς, κάτι άλλωστε που είναι δεκτό από την εφαρμογή μας. Αν όμως οι δύο αυτοί ρυθμοί είναι διαφορετικοί τότε πρέπει να προχωρήσετε σε ένα μικρό τέχνασμα. Θα ανοίξετε το πρόγραμμα BinTerm δύο φορές, τσεκάροντας στο πρώτο την επιλογή 'from PC' (από τον PC) και διαλέγοντας τη θύρα COM1, ενώ στο δεύτερο θα τσεκάρετε την 'from SPS' (από την περιφερειακή συσκευή) μαζί με τη θύρα COM2.

Όταν η μετάδοση είναι ημιαμφίδρομη (διαδοχική χρήση των δύο αγωγών) τότε το φλιπ – φλοπ είναι εκείνο που ενημερώνει το λογισμικό για το ποιος μεταδίδει δεδομένα. Η χρήση του κυκλώματος αυτού εξασφαλίζει την καλή λειτουργία της εφαρμογής, αλλά είναι πιθανό στις υψηλές ταχύτητες μετάδοσης να παρατηρηθούν σφάλματα. Μια ακόμα δυνατότητα του λογισμικού επιτρέπει την παραγωγή ενός σύντομου ήχου κάθε φορά που καταγράφεται ένα byte. Φυσικά η επιλογή αυτή είναι χρήσιμη μόνο όταν ο ρυθμός διακίνησης των byte είναι μικρός. Για τον λόγο αυτό, ακόμα και αν εσείς την έχετε ενεργοποιήσει, τίθεται αυτόματα εκτός λειτουργίας μόλις ο ρυθμός υπερβεί ένα προκαθορισμένο όριο.

Μορφές απεικόνισης

Η καρτέλα 'Data changes' (σχ. 5) έχει και αυτή να επιδείξει μια εξαιρετικά χρήσιμη λειτουργία. Με τη βοήθεια των εικονικών ρυθμιστικών της, σας επιτρέπει να επιλέξετε την μορφή με την οποία θα εμφανίζονται τα byte στο παράθυρο απεικόνισης. Οι πιθανές μορφές είναι: ASCII, δεκαδικοί ή δεκαεξαδικοί αριθμοί. Είναι επίσης δυνατή η αντιστοίχιση των τιμών με χαρακτήρες σύμφωνα με τον κώδικα ASCII. Οι αριθμοί που θα επιλέξετε για αντιστοίχιση εμφανίζονται στο δεξιό μέρος του παραθύρου, κάτω από το σχόλιο 'selected items' (επιλεγμένοι χαρακτήρες).

Όταν 'γεμίσει' μια γραμμή του παράθυρου απεικόνισης χαρακτήρων 'από τον PC' εμφανίζεται το μήνυμα 'text at line-end PC'. Ανάλογο μήνυμα, το 'text at line-end SPS', θα εμφανισθεί στην περίπτωση που συμβεί το ίδιο από την μεριά της περιφερειακής συσκευής.

Επίλογος

Κάνοντας κλικ στην καρτέλα 'Info' εμφανίζεται το όνομα, η ηλεκτρονική διεύθυνση και η δικτυακός τόπος του συγγραφέα στο Διαδίκτυο. Στις σελίδες του τόπου θα βρείτε και την εφαρμογή BinTerm. Ο συγγραφέας θα εκτιμήσει κάθε υπόδειξη και θα απαντήσει σε πάσης φύσεως ερωτήσεις σχετικές με την κατασκευή. (010041-1)