Τρελές ταχύτητες κατά παραγγελία

Από τον Henk Dijkstra

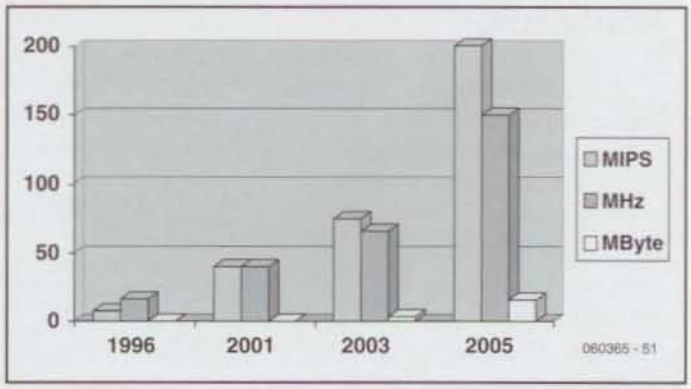
Η βελτίωση των σύγχρονων αυτοκινήτων στο ηλεκτρονικό συνεργείο

Στον κόσμο της βελτίωσης των κινητήρων, τα γαλλικά κλειδιά και τα κατσαβίδια έχουν αντικατασταθεί από φορητούς ή επιτραπέζιους υπολογιστές και ρουτίνες προγραμματισμού μνημών flash. Στην σημερινή εποχή δεν χρειάζεται να ανοίξουμε ούτε το καπό αλλά ούτε και την κεντρική μονάδα. Μέσω του συνδέσμου ODB ένα ήσυχο αυτοκίνητο μπορεί να μετατραπεί σε ένα σπορθηρίο

Είναι γνωστό σε όλους ότι τα σύγχρονα αυτοκίνητα είναι γεμάτα "μέχρι τα μπούνια" με ηλεκτρονικά. Την εποχή του 1990 δεν υπήρχαν παρά μία με δύο ηλεκτρονικές μονάδες σε κάθε όχημα, ενώ σήμερα ο αριθμός αυτός έχει φθάσει τις 10 έως 50 (ή και περισσότερες). Πέρα από τον ελεγκτή του κινητήρα και του ABS, έχουμε πλέον το δίκτυο του πίνακα οργάνων, τον ελεγκτή του κλιματιστικού, και διάφορα άλλα. Εκτός αυτού όμως, έχουμε και μία δραματική αύξηση στην διαθέσιμη υπολογιστική ισχύ (δείτε το Σχήμα 1).

Η ανάγκη για μεγαλύτερη υπολογιστή ισχύ στο αυτοκίνητο, επιβάλλεται κυρίως από τις αυξανόμενες απαιτήσεις σχετικά με τους περιορισμούς στην εκπομπή καυσαερίων και τις διαγνωστικές δυνατότητες. Ειδικά μάλιστα οι κινητήρες άμεσου ψεκασμού, απαιτούν υψηλή υπολογιστική ισχύ λόγω της πολυφασικής μορφής του ψεκασμού που χρησιμοποιούν. Ένα παράδειγμα των ενεργειών και των διεργασιών στις οποίες πρέπει να ανταποκριθεί μία Ηλεκτρονική Μονάδα Ελέγχου (Electronic Control Unit, ECU) περιγράφεται στο Σχήμα 2. Μερικά από τα ολοκληρωμένα που είναι πολύ πιθανό να βρούμε σε μία ECU είναι:

- ένας σταθεροποιητής τάσης και ενδεικτικό του επεξεργαστή
- ένα ολοκληρωμένο οδήγησης με ενδιάμεσο διαγνωστικών SPI και είσοδο SPI ή PWM
- ένα ολοκληρωμένο ενδιάμεσο διαύλου CAN
- μικροελεγκτή 8 ψηφίων στα 2 MHz με ενσωματωμένα 8 kilobyte μνήμης φλας



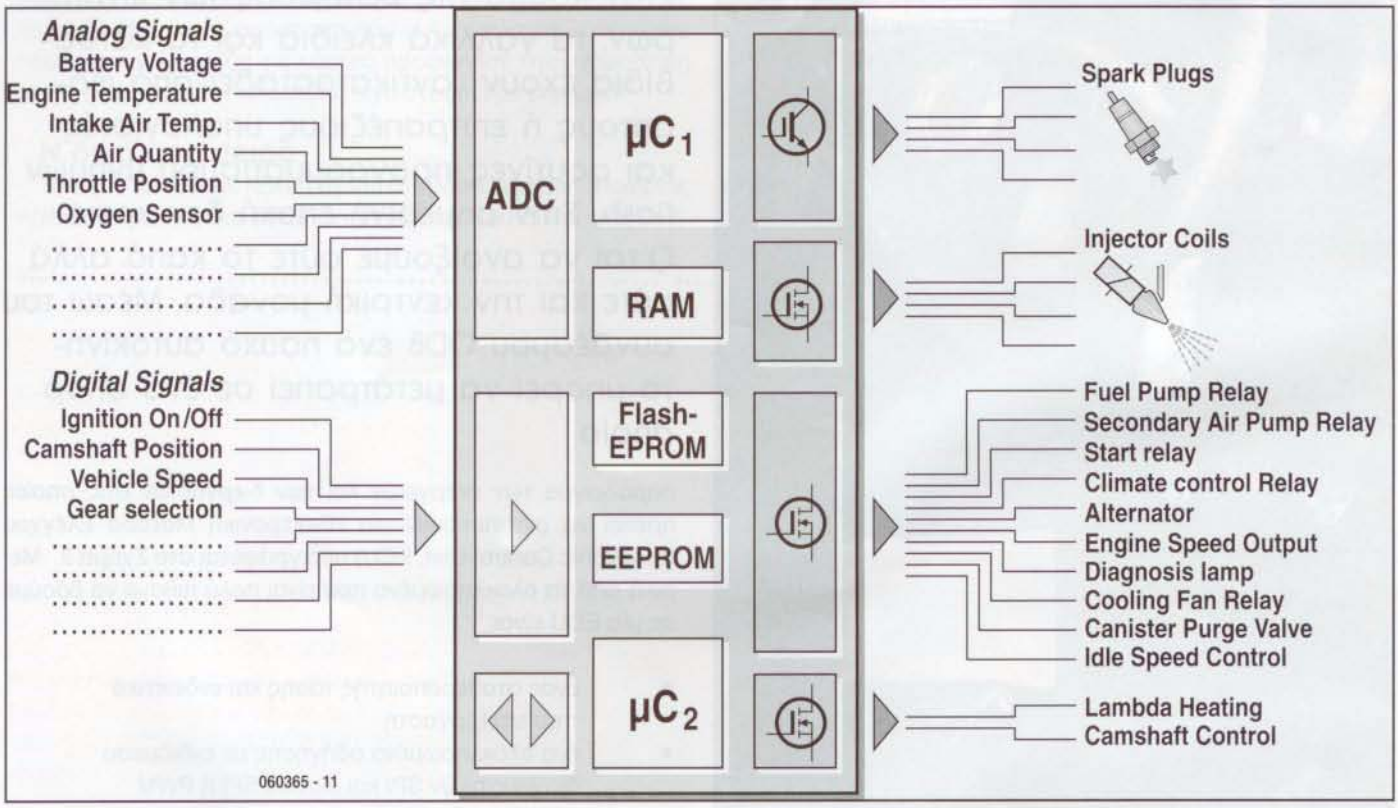
Σχήμα 1. Το μέσο πλήθος των MIPS (εντολές ανά δευτερόλεπτο X 10^6) στους μικροελεγκτές που χρησιμοποιούνται στις ECU.

Το πρότυπο J2534

Το πρότυπο J2534 αναπτύχθηκε με σκοπό να δώσει την δυνατότητα προγραμματισμού οχημάτων σε συνεργεία τα οποία δεν ανήκουν σε αλυσίδες μεγάλων κατασκευαστικών εταιρειών ("εξουσιοδοτημένα"), χωρίς αυτά να είναι υποχρεωμένα να επενδύσουν σε ακριβό και εξειδικευμένο εξοπλισμό.

Είναι πολύ πιθανόν κάποια στιγμή να χρειαστεί μία ενημέρωση του λογισμικού της ECU, έτσι ώστε το όχημα να παραμείνει σύμφωνο με τις απαιτήσεις περιορισμού αερίων ρύπων. Το συγκεκριμένο πρότυπο διευκολύνει την κατάσταση, αλλά δυστυχώς δεν το υποστηρίζουν (ακόμη) όλοι οι κατασκευαστές.

Το J2534 καλείται συχνά και ως "πρότυπο παράκαμψης". Για να μπορέσει κανείς να προγραμματίσει την ECU χρειάζεται το κατάλληλο λογισμικό από τον κατασκευαστή καθώς επίσης και το υλικό που είναι συμβατό με το πρότυπο J2534. Το πλήθος των κατασκευαστών που υποστηρίζουν το J2534 αυξάνει χρόνο με τον χρόνο. Για να προμηθευτεί κανείς το λογισμικό, συχνά αρκεί μία επίσκεψη στον δικτυακό τόπο του κατασκευαστή, όπως για παράδειγμα στην Honda όπου η διεύθυνση είναι: http://techinfo.honda.com/rjanisis/RJAAI001_tools2.asp?home=Y



Σχήμα 2. Ο ελεγκτής των μερών του κινητήρα. Το σύνολο των αισθητήρων που παρακολουθεί αυξάνει διαρκώς.

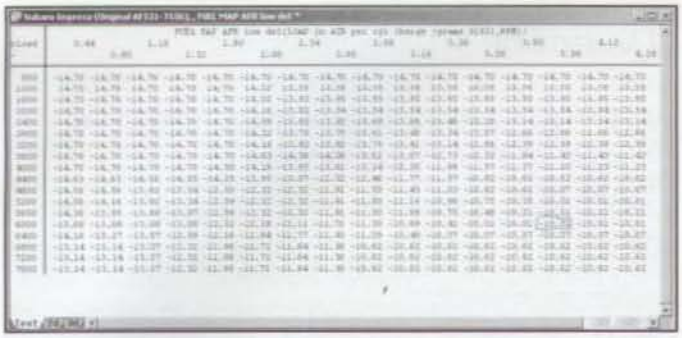
Νομοθεσία

Ο κατασκευαστής του αυτοκινήτου είναι υποχρεωμένος από τον νόμο να πάρει διάφορα προστατευτικά μέτρα έτσι ώστε ο μη εξουσιοδοτημένος προγραμματισμός του ελεγκτή να μην είναι εφικτός. Το σκεπτικό της υποχρέωσης αυτής είναι βασικά για να μην έχουμε αύξηση στις εκπομπές αερίων ρύπων. Σε πολλές όμως περιπτώσεις (όπως για παράδειγμα όταν έχουμε αλλαγές λόγω αλλαγής της εξάτμισης), επιβάλλεται να τροποποιήσουμε τις ρυθμίσεις της ECU για να παραμείνουμε σύμφωνοι με τις απαιτήσεις εκπομπής ρύπων.

Η επίσημη τροποποίηση του προγράμματος μπορεί να απαγορεύεται, αλλά στην ουσία χρειάζεται για να ρυθμίσουμε το μείγμα καυσίμου/αέρα στην σωστή αναλογία.

Είναι για παράδειγμα γνωστό σε πολύ κόσμο ότι το Subaru Impreza έρχεται από το εργοστάσιο ρυθμισμένο με αρκετά πλούσιο μείγμα και μία μικρή "ηλεκτρονική παρέμβαση" θα μπορούσε να το οδηγήσει όχι μόνον σε περισσότερη ισχύ, αλλά και -στην περίπτωση χαμηλού σχετικού φορτίου- σε μικρότερη κατανάλωση καυσίμου άρα και λιγότερες εκπομπές CO2!

Οποιαδήποτε πάντως παρέμβαση γίνει στον κινητήρα του αυτοκινήτου, είναι υποχρεωτικός ο έλεγχος από τα ΚΤΕΟ για να διευκρινιστεί εάν είναι κατάλληλο ή όχι για να κυκλοφορά στον δρόμο.



Σχήμα 3. Ενα παράδειγμα Πίνακα καυσίμου

Σχήμα 4. Προγραμματισμός ενός Subaru με φορητό προγραμματιστή από την www.fastchip.nl

- και ένα μικροελεγκτή 32 ψηφίων στα 40 MHz με ενσωματωμένα 2 MB μνήμης φλας

Προγραμματισμός ECU

Για να βελτιώσουμε τις επιδόσεις του κινητήρα μπορούμε να παρέμβουμε ηλεκτρονικά στον ελεγκτή του κινητήρα. Οι επαγγελματίες του είδους με την εξειδίκευση και την εμπειρία που διαθέτουν είναι σε θέση να τροποποιήσουν τις παραμέτρους και τους Πίνακες που βρίσκονται αποθηκευμένοι στην ECU. Οι τροποποιήσεις όμως αυτές επιβάλλουν ρύθμιση του ελεγκτή από την αρχή. Μία μετατροπή στο σύστημα εισαγωγής/εξαγωγής τροποποιεί την αναπνοή του κινητήρα σε τέτοιο βαθμό όπου είναι πιθανόν να μην είναι πλέον συμβατός με τα όρια εκπομπών ρύπων που επιβάλλει η νομοθεσία. Οι εργοστασιακές ρυθμίσεις είναι σε τελική ανάλυση βασισμένες σε ένα τυπικό σύστημα εισαγωγής εξαγωγής.

Την στιγμή που οδηγείται στον κινητήρα περισσότερος αέρας, επιβάλλεται η παροχή περισσότερου καυσίμου σε αυτόν (τουλάχιστον αυτός είναι ο σκοπός εφ' όσον απαιτείται περισσότερη ισχύς).

Το ποσό του καυσίμου που πρέπει να παρασχεθεί αποφασίζεται από την ECU, και προκύπτει από ένα πίνακα αναφοράς στον οποίο περιγράφονται οι ακόλουθες βασικές παράμετροι (δείτε το Σχήμα 3):

- φορτίο κινητήρα
- ταχύτητα κινητήρα
- θερμοκρασία κινητήρα

Στον κατακόρυφο (Y) άξονα βρίσκουμε την ταχύτητα περιστροφής του κινητήρα και στον οριζόντιο (X) το φορτίο του κινητήρα. Η θερμοκρασία αναφέρεται σε ένα άλλο πίνακα. Εάν πάρουμε σαν παράδειγμα ένα κινητήρα με ταχύτητα περιστροφής 6000 στροφές το λεπτό (rpm, revolutions per minute) και 3,96 γραμ. αέρα ανά κύλινδρο. Όπως μπορούμε να δούμε η τιμή AFR είναι 10,01. Στην συγκεκριμένη κατά συνέπεια περίπτωση, θέλουμε 1 μέρος καυσίμου για 10 μέρη αέρα. Εάν λοιπόν βάλουμε στον πίνακα την τιμή 9, τότε ο ενεργός χρόνος ψεκασμού θα αυξηθεί με σκοπό να έχουμε ένα πιο πλούσιο μείγμα στον κύλινδρο.

Είναι προφανές ότι οι σωστές τιμές είναι αυτές που αποτρέπουν αδικαιολόγητες φθορές στον κινητήρα και διατηρούν την καύση σε συμφωνία με τους κανόνες περιορισμού εκπομπής αερίων ρύπων.

Προγραμματισμός μέσω OBD

Ο προγραμματισμός των πινάκων της ECU δεν είναι απλή υπόθεση. Παλαιότερα αρκούσε η αφαίρεση της (E)PROM και αντικατάσταση αυτής με μία άλλη που περιελάμβανε τον νέο κώδικα. Σήμερα όλες οι μονάδες ECU είναι εξοπλισμένες με μνήμη φλας, η οποία μπορεί να αποτελεί ξεχωριστό ολοκληρωμένο ή όχι. Η πρόσβαση στην μνήμη της ECU γίνεται πάντοτε μέσω του συνδέσμου OBD. Για να έχουμε όμως πρόσβαση θα πρέπει πρώτα η ECU να μεταπέσει σε μία ειδική-ασφαλισμένη κατάσταση, στην οποία για να εισέλθουμε θα πρέπει να διαθέτουμε το κατάλληλο "κλειδί". Σε πολλές περιπτώσεις υπάρχουν περισσότερα του ενός επίπεδα ασφάλειας. Για κάποια τέλος αυτοκίνητα διατίθενται έτοιμες λύσεις με την μορφή φορητού προγραμματιστή.

Υλικό και λογισμικό

Το υλικό αναλαμβάνει την σωστή επικοινωνία μεταξύ του λογισμικού και της ECU κατά τον προγραμματισμό. Είναι λοιπόν προφανές ότι το υλικό θα πρέπει να διαθέτει την κατάλληλη διεπαφή, όπως για παράδειγμα είναι οι ISO, CAN, κ.λ.π. καθώς επίσης και μη τυπικούς ρυθμούς μεταφοράς δεδομένων όπως οι 10.400 ή 15.625 baud (bits/s). Σε ορισμένες περιπτώσεις απαιτείται η παρουσία και κάποιας τάσης προγραμματισμού. Στην πλειονότητα πάντως των περιπτώσεων, αρκεί το τυπικό

υλικό της ενδιάμεσο OBD. Εάν ο κατασκευαστής του αυτοκινήτου υποστηρίζει το πρότυπο J2534, αρκεί η προμήθεια μίας ενδιάμεσου J2534. Για παράδειγμα δείτε την παραπομπή [1]. Το λογισμικό διατίθεται συνήθως από τον κατασκευαστή (δείτε επίσης το ένθετο πλαίσιο κειμένου "πρότυπο J2534"). Το λογισμικό προγραμματισμού κάνει χρήση των καταστάσεων συντήρησης, όπως περιγράφονται στο πρότυπο SAE J2190 "Enhanced E/E Diagnostic Test Modes", δείτε το [2].

Οι πλέον συνήθεις καταστάσεις συντήρησης για επανα-προγραμματισμό είναι:

$10 εκκίνηση διάγνωσης
$20 παύση διάγνωσης
$27 αίτηση πρόσβασης σε ασφαλή κατάσταση (κλειδί)
$34 αίτηση μεταφοράς δεδομένων προς τον ελεγκτή
$35 αίτηση μεταφοράς δεδομένων από τον ελεγκτή
$36 μεταφορά δεδομένων από και προς τον ελεγκτή
$37 αίτηση εξόδου από μεταφορά
$3D εγγραφή στην μνήμη

Παρότι οι καταστάσεις συντήρησης περιγράφονται στο πρότυπο SEA J2190 "Enhanced E/E Diagnostic Test Modes", οι ταυτότητες των παραμέτρων (PID) ορίζονται από τον κατα-

σκευαστή. Αυτός καθορίζει την σειρά προγραμματισμού και την ασφάλεια πρόσβασης σύμφωνα με τις απαιτήσεις του.

Σύμφωνα λοιπόν με τα παραπάνω, ο κωδικός ασφαλείας θα μπορούσε να έχει μήκος 32 ψηφία, αλλά θα μπορούσε επίσης να έχει μήκος και 128 ψηφία.

Ανάστροφη μηχανική (ή αλλιώς σπάσιμο κώδικα) [Reverse engineering]

Στην περίπτωση όπου ο κατασκευαστής δεν προτίθεται να παράσχει τις αναγκαίες πληροφορίες, και την ίδια στιγμή δεν διαθέτει κάποιο λογισμικό προγραμματισμού, η μόνη επιλογή που απομένει είναι το "σπάσιμο" του κώδικα στο λογισμικού του ελεγκτή (ευτυχώς, υπάρχουν πάντα και οι κατασκευαστές οι οποίοι έχουν την πρόθεση να παράσχουν λογισμικό προγραμματισμού έτσι ώστε να είναι δυνατή η τροποποίηση των ECU).

Η διαδικασία αυτή απαιτεί την χρήση ενός αποκωδικοποιητή κατάλληλου για τον συγκεκριμένο επεξεργαστή, και μίας αντίστοιχης διεπαφής. Δεδομένου ότι όλη η ανάλυση είναι απα-

Γλωσσάρι

AFR (Air Fuel Ratio, Λόγος καυσίμου αερίου).
Ο λόγος μεταξύ καυσίμου και αέρα

CAN-bus (Controller Area Network, Δίκτυο περιοχής ελεγκτή).
Ένα ασύγχρονος σειριακός δίαυλος σχεδιασμένος για χρήση στο αυτοκίνητο

ECU (Electronic Control Unit, Ηλεκτρονική μονάδα ελέγχου).
Ο υπολογιστής του οχήματος, ο οποίος ελέγχει όλα τα ηλεκτρονικά μέρη

MIPS (Million Instructions Per Second, Εκατομμύρια εντολές το δευτερόλεπτο).
Το πλήθος των εντολών που είναι σε θέση να εκτελέσει ο ελεγκτής στην μονάδα του χρόνου (για παράδειγμα η πρόσθεση δύο αριθμών σε μία εντολή).

PWM (Pulse Width Modulation, Διαμόρφωση κατά πλάτος παλμού).
Διαμόρφωση της διάρκειας του παλμού προς περιοδο σε μια παλμοσειρά που περιέχει την πληροφορία του σήματος.

OBD (On-Board Diagnostic, Διαγνωστικό επί του οχήματος).
Ηλεκτρονικό διαγνωστικό σύστημα αυτοκινήτων.

SPI (Serial Peripheral Interface, Περιφερειακή σειριακή διεπαφή).
Πρότυπο σειριακής διασύνδεσης για δίκτυο ψηφιακού σήματος. Εάν η συσκευή κάνει τη δουλειά για την οποία φτιάχτηκε, ο σκοπός έχει πραγματοποιηθεί. Εσείς, θα πρέπει απλώς, να φροντίσετε για τις ...αδυναμίες της.

Οι εποχές όπου ο μηχανικός λέρωνε τα χέρια για να ρυθμίσει τον κινητήρα έχουν παρέλθει...

Για να μπορέσουμε λοιπόν να ανακαλύψουμε την σειρά προγραμματισμού και να αποκτήσουμε δικαιώματα πρόσβασης στον επεξεργαστή, θα πρέπει να αναλύσουμε τον κώδικα. Η διαδικασία αυτή απαιτεί την χρήση ενός αποκωδικοποιητή κατάλληλου για τον συγκεκριμένο επεξεργαστή, και μίας αντίστοιχου ενδιάμεσου. Δεδομένου ότι όλη η ανάλυση είναι απαραίτητο να γίνει σε επίπεδο συμβολικής γλώσσας (assembly), έχουμε να κάνουμε με μία δουλειά η οποία μπορεί να αποδειχθεί ιδιαίτερα χρονοβόρα. Ανάλογα μάλιστα με τον τρόπο που υλοποιεί τις διαδικασίες ο κατασκευαστής, είναι πιθανόν να χρειαστεί να φτιάξουμε και κάποιο πυρήνα ή και κάποιες ρουτίνες προγραμματισμού μνημών φλας από την αρχή. Κατά συνέπεια, όλη αυτή η δουλειά δεν μπορεί σε καμία περίπτωση να γίνει από κάποιον αρχάριο.

Το αυτοκίνητο απέναντι στους υπολογιστές

Στην σημερινή εποχή το "πείραγμα" των αυτοκινήτων δείχνει περισσότερο με "hacking" παρά με δουλειά στο συνεργείο. Λόγω της εκτεταμένης χρήσης ηλεκτρονικών συστημάτων, ένα διαρκώς αυξανόμενο πλήθος ρυθμίσεων γίνεται με ηλεκτρονικά μέσα. Για λόγους ασφαλείας αλλά και για να είναι σύμφωνοι με τις διάφορες νομικές απαιτήσεις, οι κατασκευαστές κλειδώνουν το λογισμικό όσο το δυνατόν περισσότερο. Από την άλλη υπάρχουν αρκετές εταιρείες ρύθμισης αυτοκινήτων (όπως για παράδειγμα η Fastchip), οι οποίες είναι απασχολημένες με το σπάσιμο του κώδικα για να είναι σε θέση να κάνουν οι ίδιες τις "ρυθμίσεις" που θέλουν. Το σκηνικό αυτό μοιάζει λίγο με το έργο που παίζεται στην αρένα των προγραμμάτων για προσωπικούς υπολογιστές (για παράδειγμα οι χάκερ που σπάνε τους μηχανισμούς προστασίας για να έχουν την δυνατότητα να πάρουν ένα αντίγραφο του αγαπημένου τους παιχνιδιού στο Xbox...)

Όσο τα ηλεκτρονικά στο αυτοκίνητο γίνονται περισσότερο περίπλοκα τόσο θα συνεχίσει να παίζεται το ίδιο έργο, και απ' ότι φαίνεται η Τεχνολογία της Πληροφορίας (IT) θα αποκτά όλο και μεγαλύτερο ρόλο στο συνεργείο. Αυτό είναι κάτι περισσότερο από σίγουρο!

Σύνδεσμοι στο διαδίκτυο:

[1] www.passthruxs.com

[2] www.sae.org

[3] www.fastchip.nl