ΤΕΧΝΙΚΗ ΕΙΣΑΓΩΓΗΣ ΛΑΘΟΥΣ ΣΤΟ ΛΟΓΙΣΜΙΚΟ ΕΛΕΓΧΟΥ ΤΟΥ ΡΥΘΜΙΣΤΗ ΣΤΡΟΦΩΝ ΤΩΝ ΓΕΩΡΓΙΚΩΝ ΕΛΚΥΣΤΗΡΩΝ

Ιωάννης Γράβαλος
Ηρ. Πολυτεχνείου 198 Τ.Κ.41221-Λάρισα

ΠΕΡΙΛΗΨΗ

Οι κατασκευαστές γεωργικών ελκυστήρων καταβάλλουν μεγάλες προσπάθειες για να υλοποιήσουν καλωδιωμένες εφαρμογές (όπως η αυτόματη σύμπλεξη της εμπρόσθιας κίνησης κ.λπ.). Τα ενσωματωμένα συστήματα ελέγχου των εφαρμογών αυτών, πρέπει να διακρίνονται για τη μεγάλη ακρίβεια και την υψηλή αξιοπιστία τους. Για να μελετήσουμε την αξιοπιστία ενός τέτοιου συστήματος, να αναγνωρίσουμε και να καταλάβουμε τις πιθανές βλάβες του, χρησιμοποιούμε τεχνικές όπως η εισαγωγή λάθους. Στην εργασία αυτή προτείνεται ένα σύστημα εισαγωγής λάθους για τον ρυθμιστή στροφών του κινητήρα. Δίνεται έμφαση σε τεχνικές SWIFI, οι οποίες μεταβάλλουν την κατάσταση του ενσωματωμένου λογισμικού, σαν να είχε πραγματικά προσβληθεί από κάποιο λάθος.

Λέξεις κλειδιά: Γεωργικός ελκυστήρας, ρυθμιστής στροφών κινητήρα, τεχνικές εισαγωγής λάθους, αξιοπιστία.

A FAULT INJECTION SYSTEM FOR THE CONTROLLER SOFTWARE OF AGRICULTURAL TRACTOR GOVERNORS

Ioannis Gravalos
198, Iroon Polytechniou str. – 41221 Larissa

ABSTRACT

Manufacturers of agricultural tractors make great efforts to implement “by wire” applications (e.g. automatic engagement of the front wheel drive etc.). The embedded control systems involved in such applications, must be characterized by high accuracy and reliability. In order to study the reliability of such control systems and to recognize and understand their possible failure modes, we can use various fault injection techniques. In this present work, we present a fault injection system for an engine speed controller. The system is based on a SWIFI technique, which changes the state of the embedded software, as it would have happened by a real fault.

Key words: Agricultural tractor, engine speed controller, fault injection techniques, reliability.

1. ΕΙΣΑΓΩΓΗ

Στους γεωργικούς ελκυστήρες έχουμε εκτεταμένη εφαρμογή ενσωματωμένων συστημάτων (ολοκληρωμένα τμήματα μεγαλυτέρων συστημάτων), τα οποία ελέγχουν κρίσιμες λειτουργίες όπως για παράδειγμα τον αριθμό στροφών του κινητήρα.

Το ενσωματωμένο λογισμικό τους, πρέπει να διακρίνεται για τη μεγάλη ακρίβεια και την υψηλή αξιοπιστία. Η μη έγκαιρη ανακάλυψη λαθών είναι δυνατόν να οδηγήσει σε σημαντικές απώλειες.

Η εισαγωγή λάθους (fault injection) είναι μία μέθοδος που χρησιμοποιείται συχνά για να επιβεβαιωθεί εάν ένα σύστημα λογισμικού παρουσιάζει ανοχή σε λάθη [1].

Η αρχή βασίζεται στην εισαγωγή ενός τεχνητού λάθους στο ενσωματωμένο λογισμικό και στη συνέχεια παρατηρείται η συμπεριφορά του. Η παρουσία λάθους δεν είναι αρκετή για να προσβάλλει την αξιοπιστία ενός συστήματος. Το λάθος (fault) θα πρέπει να ενεργοποιηθεί κατά τη διάρκεια της λειτουργίας του συστήματος αυτού [2].

Οι κυριότερες τεχνικές εισαγωγής λάθους που χρησιμοποιούνται είναι:

-Η εισαγωγή λάθους στο υλικό του συστήματος προορισμού (hardware fault injection). Είναι μία δημοφιλής προσέγγιση, επειδή ανταποκρίνεται περισσότερο προς ένα πραγματικό μοντέλο λάθους. Ομως για την υλοποίησή της απαιτείται ειδικός εξοπλισμός που αυξάνει σημαντικά το κόστος.

-Η εισαγωγή λάθους που υλοποιείται σε ένα μοντέλο εξομοίωσης του συστήματος προορισμού (fault injection by simulation). Προτείνεται για διερεύνηση της αξιοπιστίας μικρότερων συστημάτων.

-Οι τεχνικές SWIFI (software implemented fault injection). Μεταβάλλουν την κατάσταση υλικού/λογισμικού του συστήματος προορισμού χρησιμοποιώντας ειδικά προγράμματα, με αποτέλεσμα να συμπεριφέρεται σαν να συνέβη ένα πραγματικό λάθος υλικού.

Τα εργαλεία SWIFI είναι σχετικά χαμηλότερου κόστους, συγκριτικά με άλλα εργαλεία υλικού (hardware tools) και για το λόγο αυτό έτυχαν ευρείας αποδοχής. Κυριότερες τεχνικές είναι:

- FIAT: (Fault Injection-based Automated Testing environment), [3].
- FTAPE: (Fault Tolerance and Performance Evaluator), [4].
- FERRARI: (Fault and Error Automatic Real-Time Injection), [5].
- DOCTOR: (IntegrateD sOftware fault injeCTiOn enviRonment), [6].
- Xception, [7].

Στην εργασία αυτή, προτείνεται ένα σύστημα εισαγωγής λάθους για θέσεις της μνήμης και επιλεγμένους καταχωρητές στο ενσωματωμένο λογισμικό ελέγχου του ρυθμιστή στροφών του κινητήρα. Το σύστημα αυτό, αποτελεί μία γενικότερη εφαρμογή εισαγωγής λάθους για τα συστήματα ελέγχου των αυτοκινούμενων γεωργικών μηχανημάτων. Τα κύρια χαρακτηριστικά του είναι: το χαμηλό κόστος, η ευκαμψία (υποστηρίζει διαφορετικούς τύπους λαθών) και η

γρήγορη προσπέλαση (μπορεί εύκολα να μετακινείται σε διευθύνσεις διαφορετικών συστημάτων προορισμού).

2. ΡΥΘΜΙΣΤΗΣ ΣΤΡΟΦΩΝ ΚΙΝΗΤΗΡΑ

Στον γεωργικό ελκυστήρα, το ηλεκτρονικό σύστημα ελέγχου των στροφών του κινητήρα εκτός του ρυθμιστή περιλαμβάνει έναν μαγνητικό λήπτη, ένα ποτενσιόμετρο που παρακολουθεί τη διαδρομή του ποδομοχλού τροφοδοσίας, ένα ψηφιακό χειριστήριο και έναν βηματικό κινητήρα (ο ρυθμιστής στροφών και το λογισμικό ελέγχου του ρυθμιστή αποτελούν δύο διαφορετικά συστήματα). Αναλυτική περιγραφή του συστήματος ελέγχου των στροφών του κινητήρα, γίνεται στις εργασίες [8], [9].

Ο ακριβής και σταθερός αριθμός στροφών του κινητήρα είναι αναγκαίος καθώς ο γεωργικός ελκυστήρας εργάζεται σε συνθήκες που χαρακτηρίζονται από μεγάλες διακυμάνσεις φορτίου. Στόχος του ρυθμιστή δύο όρων (PI) είναι η συνεχής ταύτιση των πραγματικών στροφών του κινητήρα με τις επιθυμητές στροφές, ανεξάρτητα από οποιεσδήποτε διαταραχές.

Η διαφορά ανάμεσα στις επιθυμητές y_{sp} και τις πραγματικές στροφές y είναι γνωστή ως σήμα σφάλματος e και δίνεται από τη σχέση :

$$e(t) = y_{sp}(t)-y(t) \qquad (1)$$

Ο ολοκληρωτικός όρος w του ρυθμιστή (PI) χρησιμοποιείται για την εξάλειψη του μόνιμου σφάλματος e (πολλαπλασιάζοντάς το με το ολοκληρωτικό κέρδος k_i) σύμφωνα με τη σχέση:

$$w(t) = w(t-1) +T\, k_i\, e(t) \qquad (2)$$

όπου T είναι ο χρόνος δειγματοληψίας.

Επιπροσθέτως, ο αναλογικός όρος ενισχύει το σήμα σφάλματος e με το αναλογικό κέρδος k και η επιθυμητή γωνία ρύθμισης u είναι το άθροισμα αναλογικού και ολοκληρωτικού όρου, σύμφωνα με τη σχέση :

$$u(t) = ke(t) + w(t) \qquad (3)$$

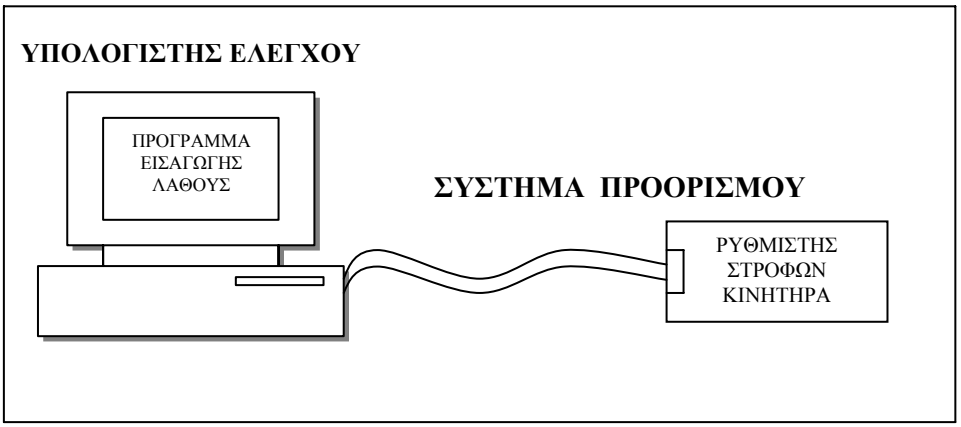
Επειδή το σήμα u(t) μπορεί να λάβει τιμές εκτός του διαστήματος ρύθμισης 0.0 °-70.0 °, μία συνάρτηση εξόδου διασφαλίζει ώστε το σήμα u' να κυμαίνεται πάντα εντός αυτού.

3. ΤΕΧΝΙΚΗ ΕΙΣΑΓΩΓΗΣ ΛΑΘΟΥΣ

Οπως παρατηρούμε στο σχήμα 1, η πειραματική διάταξη που χρησιμοποιήσαμε, περιλαμβάνει ένα εργαλείο εισαγωγής λάθους εγκατεστημένο στον υπολογιστή και το λογισμικό ελέγχου του ρυθμιστή του κινητήρα στη θέση του συστήματος προορισμού.

Για την εκτέλεση των πειραμάτων, επιλέχθηκε η τελευταία έκδοση ενός εμπορικού εργαλείου εισαγωγής λάθους, που προσαρμόζεται εύκολα σε διαφορετικά συστήματα προορισμού και διαφορετικές τεχνικές. Είναι γραμμένο σε γλώσσα Java και χρησιμοποιεί μια βάση SQL για την αποθήκευση των δεδομένων.

Η χρήση του συστήματος είναι απλή και επιβεβαιώνεται από τη διαδικασία της εγκατάστασης και της ρύθμισης. Βασικά περιλαμβάνει τρεις φάσεις : τη φάση προετοιμασίας, τη φάση εισαγωγής και τη φάση ανάλυσης.



Σχήμα 1: Πειραματική διάταξη συστήματος εισαγωγής λάθους.

3.1 Φάση προετοιμασίας

Στη φάση της προετοιμασίας εμφανίζονται στη γραφική διασύνδεση του χρήστη (graphical user interface-GUI), οι παράμετροι του συστήματος προορισμού. Επίσης, ο χρήστης έχει τη δυνατότητα να επιλέξει από το αρχείο λαθών, που εμφανίζεται σε ένα παράθυρο, τις θέσεις και τον τύπο λάθους. Τα δεδομένα αυτά αποθηκεύονται σε μία βάση που αποκαλείται Campaign Data. Προβλέπεται η τροποποίηση ενός λάθους όταν : (α) το λάθος αποδεδειγμένα δεν επηρεάζει τη συμπεριφορά του συστήματος προορισμού και (β) ένα λάθος είναι ισοδύναμο ενός άλλου.

3.2 Φάση εισαγωγής

Πρόκειται για τη σημαντικότερη φάση της όλης διαδικασίας εισαγωγής λάθους.

Αρχικά ο αλγόριθμος (fault injection algorithm) διαβάζει το περιεχόμενο της βάσης δεδομένων (Campaign Data). Στη συνέχεια προκαλεί την εκτέλεση του προγράμματος αρχικοποίησης (initialization) στο σύστημα προορισμού, με στόχο να διασφαλιστεί ένα περιβάλλον χωρίς λάθη. Η εκτέλεση χωρίς λάθη (reference execution) του λογισμικού, υποφορτώνεται στη βάση δεδομένων (Logged System State). Κατόπιν, ο αλγόριθμος αναζητά τα ανοικτά σημεία του υποφορτομένου κώδικα, στον οποίο πρόκειται να εισάγει το περιεχόμενο της

βάσης Campaign Data. Μετά την εισαγωγή λάθους, η εκτέλεση του λογισμικού στο σύστημα προορισμού αρχίζει από το σημείο που είχε σταματήσει και συνεχίζεται μέχρι έως ότου ολοκληρωθεί. Το αποτέλεσμα αποθηκεύεται στη βάση Logged System State. Πριν την έναρξη του επόμενου κύκλου εισαγωγής, έχουμε επανεκκίνηση του συστήματος προορισμού.

Κατά τη διάρκεια της εισαγωγής λάθους, ο χρήστης έχει τη δυνατότητα να παρακολουθεί στην οθόνη του υπολογιστή την εξέλιξη του πειράματος. Πληροφορείται τον αριθμό λαθών που έχουν εισαχθεί και μπορεί να διακόψει, επανεκκινήσει ή να τελειώσει τη διαδικασία.

3.3 Φάση ανάλυσης

Κατά τη φάση αυτή, αναλύονται τα δεδομένα που αποθηκεύτηκαν στη βάση Logged System State, με σκοπό να επιτευχθεί η ταξινόμηση των βλαβών σε κατηγορίες και να διαμορφωθούν διάφορα κριτήρια αξιοπιστίας για το σύστημα προορισμού που μελετάται.

4. ΑΠΟΤΕΛΕΣΜΑΤΑ ΠΕΙΡΑΜΑΤΩΝ

Για τη πειραματική επαλήθευση της αποτελεσματικότητας του προτεινόμενου συστήματος εισαγωγής λάθους, επιλέχθηκε για σύστημα προορισμού ο ρυθμιστής στροφών του κινητήρα του γεωργικού ελκυστήρα Lamborghini Formula 135 VDT. Ο ρυθμιστής στροφών τύπου REG 2MFA, κατασκευάστηκε από την S.M.E. s.r.l. Arzignano (VI) Italy. Ο συγκεκριμένος ρυθμιστής έχει ενσωματωμένο τον μικροεπεξεργαστή TN 80C198-16 της Intel. Πρόκειται για έναν μικροεπεξεργαστή τεχνολογίας CMOS των 16 bit στα 16 MHz.

Για να εγκατασταθεί το λογισμικό του συστήματος εισαγωγής λάθους, επιλέχθηκε υπολογιστής (host computer) ένα PC με επεξεργαστή Pentium 4/1,9 GHz και λειτουργικό MS Win. 2000.

Οι βλάβες που επηρεάζουν την έξοδο του ρυθμιστή διακρίνονται σε τρεις μεγάλες κατηγορίες:

- μόνιμες (permanent): η έξοδος του ρυθμιστή λαμβάνει τη μέγιστη τιμή (70.0 °) ή την ελάχιστη (0.0 °) από τη στιγμή εμφάνισης της βλάβης έως την ολοκλήρωση του χρόνου παρατήρησης.
- Ημιμόνιμες (semipermanent): η έξοδος του ρυθμιστή διαφοροποιείται έντονα κατά τη διάρκεια περισσοτέρων από μίας εκτελέσεων και επανέρχεται στην κατάσταση χωρίς λάθος έγκαιρα και εντός του χρόνου παρατήρησης.
- παροδικές (transient): η έξοδος του ρυθμιστή διαφοροποιείται έντονα κατά τη διάρκεια μίας εκτέλεσης και αμέσως επανέρχεται στην κατάσταση χωρίς λάθος. Οι βλάβες αυτές έχουν ελάχιστη επίδραση στην ελεγχόμενη διαδικασία.

Η εισαγωγή λαθών στην CPU αφορά τους καταχωρητές γενικής χρήσης, τον μετρητή προγράμματος και τον δείκτη σωρού. Τα λάθη στους ανωτέρω καταχωρητές έχουν μεγαλύτερες πιθανότητες διάδοσης. Η εισαγωγή λαθών στη μνήμη έγινε απευθείας σε επιλεγμένες θέσεις, τροποποιώντας το περιεχόμενό

τους. Τα λάθη που χρησιμοποιήθηκαν για τους καταχωρητές και τη μνήμη ήταν απλά bit-flips.

Στη συνέχεια παρατίθενται τα αποτελέσματα των πειραμάτων εισαγωγής 2.437 λαθών.

Πίνακας 1: Αποτελέσματα των πειραμάτων εισαγωγής λάθους.

Τμήματα της CPU	**Μνήμη** (2005)		**Καταχωρητές** (432)	
Κατηγορίες βλαβών	**%**	**Λάθη**	**%**	**Λάθη**
Μόνιμες	0.05	1	0.46	2
Ημιμόνιμες	0.10	2	0.46	2
Παροδικές	25.59	513	4.40	19
Χωρίς λάθος	74.26	1489	94.68	409
Σύνολο	100	2005	100	432

Οι δύο στήλες του πίνακα δίνουν τα αποτελέσματα χωριστά για λάθη που εισήχθησαν στα δεδομένα της μνήμης και στους καταχωρητές της CPU. Παρουσιάζεται το ποσοστό για κάθε κατηγορία βλάβης καθώς και ο αριθμός των λαθών.

Από τα αποτελέσματα γίνεται φανερό ότι μόνο το 0,28% του συνόλου των λαθών εισαγωγής είχαν σοβαρή επίδραση στο σημείο εξόδου του ρυθμιστή. Αντιθέτως, το 99,72% των λαθών είχε ελάχιστη έως καμία επίδραση στη λειτουργία του. Επίσης προκύπτει ότι σοβαρές βλάβες προκλήθηκαν περισσότερο από την εισαγωγή bit-flips στους καταχωρητές της CPU.

Ενας τρόπος για να αποφύγουμε τα αποτελέσματα των bit-flips είναι η χρήση εκτελούμενων βεβαιώσεων (executable assertions) στο λογισμικό ελέγχου του ρυθμιστή στροφών.

5. ΣΥΜΠΕΡΑΣΜΑΤΑ

1. Η εισαγωγή bit-flips στους καταχωρητές της CPU κατά την εκτέλεση του λογισμικού ελέγχου του ρυθμιστή, μπορεί να προκαλέσει μόνιμες βλάβες.
2. Σοβαρή επίδραση στην έξοδο του ρυθμιστή είχε μόνο το 0,28% του συνόλου των λαθών που εισήχθησαν.
3. Αντιθέτως, το 99,72% των εισαχθέντων λαθών είχε ελάχιστη έως καμία επίδραση στη λειτουργία του ρυθμιστή.
4. Το προτεινόμενο σύστημα εισαγωγής λάθους δεν απαιτεί ιδιαίτερο εξοπλισμό, υποστηρίζει διαφορετικούς τύπους λαθών και είναι σχετικά χαμηλού κόστους.
5. Η τεχνική εισαγωγής λάθους στο λογισμικό ελέγχου παρέχει τη δυνατότητα διερεύνησης της αξιοπιστίας σε πολλές εφαρμογές των μικροελεγκτών (όπως αυτές των αυτοκινούμενων γεωργικών μηχανημάτων).

6 . ΒΙΒΛΙΟΓΡΑΦΙΑ

1. Lai, M.Y., Wang, S.Y., 1995. *Software fault tolerance*. John Wiley & Sons Ltd.
2. Arlat, J., Aguera, M., Amat, L., Crouzet, Y., Fabre, J. C., Laprie, J. C., Martins, E., Powell, D., 1990. Fault injection for dependability validation: A methodology and some applications. *IEEE Trans. On Software Eng.,* 16, (2), 166-182.
3. Segall, Z., Vrsalovic,D., Siewiorek, D., Yaskin, D., Kownacki, J., Barton, J., Rance Y.D., Robin, A., Lin, T., 1998. FIAT: Fault injection based automated testing environment. *Proc. 18th Int. Symp. on FT Computing (FTCS-18)* 102-107.
4. Tsai, T.K., Lyer, R.K, 1993. An approach to benchmarking of fault-tolerant commercial system. *Proc. 26th Ann. Int. symp. FT Computing. IEEE CS Press,* Los Alamitos, calif., 314-323.
5. Kanawati, G.A., Kanawati, N.A., Abraham, J.A., 1992. FERRARI: A tool for the validation of system dependability properties. *Proc. 22nd Ann. Int. Symp. FT Computing. IEEE CS Press*, Los Alamitos, Calif., 336-344.
6. Han, S., Shin, K.G., Rosenberg, H.A.,1995. Doctor: integrated software fault injection environment for distributed real-time systems. *Proc. 2nd Ann. IEEE Int. Comp. Perf. and Dep. Symp.,* Los Alamitos, Calif., 204-213.
7. Carreira, J., Madeira, H., Silva, J., 1998. Xception: A technique for the experimental evaluation of dependability in modern computers. *IEEE Trans. On Software Eng.,* 24, 125-136.
8. Smith, L.A., 1989. Precise control of tractor engine speed. *Transactions of the ASAE,* 32, (2), 385-389.
9. Gravalos, I., 1990. *Navrh mericich a ridicich systemu v zemedelstvi.* Pisemna prace k odborne Kandidatske Zkousce. VSZ v Praze 3-27.