Λειτουργικά Συστήματα Πραγματικού Χρόνου
2006-07

Ασφαλή Συστήματα

Μέθοδοι ελέγχου και εξακρίβωσης ορθής λειτουργίας

Μ.Στεφανιδάκης

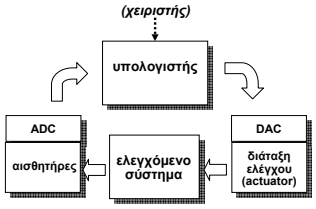
Ενσωματωμένα Συστήματα: Απαιτήσεις

- Αξιοπιστία (reliability)
- Χρηστικότητα (usability)
- Προσαρμοστικότητα (adaptability)
  - Χρήση από μη ειδικευμένους χειριστές
  - Σε απροσδιόριστες συνθήκες
- Ασφάλεια (safety)
  - Safety-critical systems
    - Οχήματα
    - Αεροσκάφη
    - Ιατρικά μηχανήματα
    - ...

Ασφάλεια: βασικές έννοιες

- Η έννοια του "ατυχήματος"
  - Μη αναμενόμενη σειρά γεγονότων
  - Με αποτέλεσμα
    - Βλάβη ζωής
    - Βλάβη περιουσίας ή εξοπλισμού
    - Βλάβη περιβάλλοντος
- Κίνδυνος "ατυχήματος"
  - Σοβαρότητα
  - Πιθανότητα εκδήλωσης
- Αδυναμία αποκλεισμού ατυχήματος!
  - Μόνο μείωση του κινδύνου ατυχήματος
    - Με αύξηση του κόστους του συστήματος

Τμήματα εφαρμογής ελέγχου



- Πιθανότητα αστοχίας
  - Σε οποιοδήποτε από τα εμπλεκόμενα μέρη

Ασφαλείς εφαρμογές

- Fail-safe
  - Άμεση αναγνώριση σφαλμάτων
    - Από υλικό, λογισμικό ή χειριστή
  - Αντίδραση σε σύντομο χρόνο
    - Πριν να επηρεαστεί η συμπεριφορά του συστήματος
  - Μετάβαση σε "ασφαλή κατάσταση" (safe state)
    - Γενικά: μη λειτουργική κατάσταση!!
- Fail-operational
  - Συνέχιση παροχής κρίσιμης υπηρεσίας
    - Μετά από την εμφάνιση σφάλματος
    - Πιθανώς: με υποβαθμισμένη ποιότητα
  - Π.χ.: έλεγχος πτήσης αεροσκαφών

Σφάλματα

- Οδήγηση συστήματος σε εσφαλμένη κατάσταση
- Είδη σφαλμάτων
  - Τυχαία – Σκόπιμα
  - Φυσικά – Λόγω σχεδιασμού
  - Εσωτερικά – Εξωτερικά
    - Από αστοχία συστήματος ή εξωτερικούς παράγοντες
  - Προσωρινά – Μόνιμα
    - Πιθανώς: μόνιμη κατάσταση στο σύστημα
    - Αναγκαιότητα εξωτερικής επέμβασης - επισκευής

Αντιμετώπιση σφαλμάτων

- Σε επίπεδο αρχιτεκτονικής συστήματος
  - Διαφανώς ως προς την εφαρμογή
  - Σύνθετο σύστημα – πρόσθετο υλικό
- Σε επίπεδο εφαρμογής
  - Πρόσθετες λειτουργίες ανίχνευσης και διόρθωσης
  - Πολυπλοκότερο λογισμικό (εφαρμογής)

Αστοχίες λόγω σφαλμάτων

- Απόκλιση από την προσχεδιασμένη λειτουργία
  - Λόγω μετάβασης σε κατάσταση λάθους...
  - ...η οποία προκαλείται από σφάλματα
- Είδη αστοχιών
  - Υπολογιζόμενων τιμών – Χρονικές
  - Μόνιμες – Προσωρινές
  - Απλές – Καταστροφικές

Αστοχίες σε κατανεμημένα συστήματα

- Συνεκτική μετάδοση της πληροφορίας
  - Όλα τα υποσυστήματα λαμβάνουν την ίδια πληροφορία
    - fail-consistent
    - fail-silent (ορθή μετάδοση ή καθόλου)
    - fail-stop
- Μη συνεκτική μετάδοση
  - Διαφορετικά (εσφαλμένα) αποτελέσματα
    - Malicious (Byzantine) failures

Ανοχή σε σφάλματα

- Μέσω πολλαπλών ίδιων τμημάτων (replicas)
  - Για την αντιμετώπιση k αστοχιών του ίδιου τύπου χρειάζονται:
    - k+1 τμήματα (fail-silent)
      - Αντίγραφα σε αναμονή
    - 2k+1 τμήματα (fail-consistent)
      - Διαδικασία ψηφοφορίας
    - 3k+1 τμήματα (malicious)
      - Πρωτόκολλα συμφωνίας με καθολική ανταλλαγή πληροφοριών

Διόρθωση σφάλματος: exceptions

- Παρουσία σφάλματος σε διεργασία
  - Δημιουργία exception
  - Από υλικό ή λογισμικό
- Εκτέλεση ρουτίνας εξυπηρέτησης
  - Επηρεάζει τον χρόνο WCET της διεργασίας!

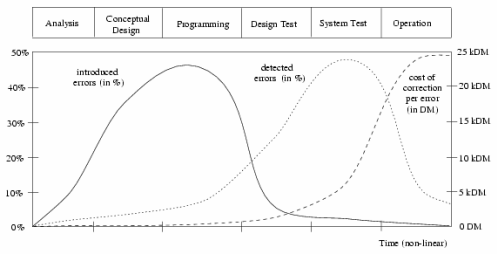
Ανάλυση συνθηκών σφάλματος

- Failure mode and Effects analysis (FMEA)
- Σε κάθε επιμέρους τμήμα του συστήματος
  - Τυχαία σφάλματα υλικού
  - Κατασκευαστικές αστοχίες
  - Προγραμματιστικά λάθη
  - Επιβάρυνση περιβαλλοντικών παραγόντων
  - Σφάλματα συντήρησης
- Διορθώσεις για τη μείωση πιθανότητας σφάλματος
  - Αύξηση ποιότητας και αξιοπιστίας τμημάτων
  - Διατάξεις ασφάλειας (εσωτερικές & εξωτερικές)

Άλλες μέθοδοι ανάλυσης

- **Fault Tree Analysis (FTA)**
  - **Ξεκινώντας από αναγνωρισμένο σφάλμα**
  - **Ανίχνευση τμημάτων που μπορούν να το προκαλέσουν**
  - **Και καθορισμός μέτρων για τον περιορισμό του**
- **(Probabilistic) Risk Analysis ([P]RA)**
  - **Ποσοτική μέθοδος**
  - **Πιθανότητα σφάλματος κάθε υποτμήματος**
    - **π.χ. ανά ώρα λειτουργίας**
  - **Εξαγωγή συνοπτικής πιθανότητας σφάλματος**

Σφάλματα ανάπτυξης



- **Πως διαπιστώνεται η ορθή λειτουργία του νέου συστήματος;**

Έλεγχος ορθής λειτουργίας

- **Σε πολλά συστήματα: το μεγαλύτερο μέρος του κύκλου ανάπτυξης!**
- **Δοκιμαστική λειτουργία (testing)**
  - **Με επιλεγμένα δεδομένα εισόδου**
  - **Για τον έλεγχο παρεχόμενων λειτουργιών**
  - **Και τήρηση χρονικών προθεσμιών**
- **Formal Methods**
  - **Μαθηματικές και λογικές τεχνικές**
  - **Για την απεικόνιση ενός συστήματος**
  - **Και την <u>απόδειξη</u> της ορθής λειτουργίας**

Testing

- **Με αντιπροσωπευτικά(;) δεδομένα εισόδου**
  - **Προσομοίωση χειρότερης περίπτωσης**
  - **Κάλυψη μέρους των πιθανών καταστάσεων λειτουργίας**
  - **Σε συνδυασμό με εξομοίωση**
- **Δυνατότητα παρατήρησης (observability)**
  - **Probe effect**
- **Σχεδιασμός για έλεγχο**
  - **Πρόβλεψη αρχιτεκτονικής για διευκόλυνση ελέγχου**
- **Αλλά:**

  "ο δοκιμαστικός έλεγχος μπορεί μόνο να δείξει την παρουσία σφαλμάτων, ποτέ όμως να αποδείξει την απουσία τους" **(Dijkstra)**

Formal Methods

- **Κατασκευή μοντέλου συστήματος**
  - **Σύνολο καταστάσεων (πληροφορία μεταβλητών κ.λ.π.)**
  - **Περιγραφή συνθηκών μεταβάσεων μεταξύ καταστάσεων**
- **Μαθηματική περιγραφή προδιαγραφών εφαρμογής**
  - **Περιορισμοί (π.χ. χρονικοί)**
- **Σύνολο λογικών κανόνων**
  - **Για την απόδειξη ότι το σύστημα τηρεί τις προδιαγραφές**

Model Checking

- Αυτοματοποιημένη απόδειξη
  - Μέσω υπολογιστικών εργαλείων
- Εξαντλητική διερεύνηση συνόλου καταστάσεων
  - Για απόκλιση από το επιθυμητό σχήμα
  - Παραβίαση προδιαγραφών- Reachability Analysis
- Σε περίπτωση αποτυχίας;
  - Παρουσίαση αντι-παραδείγματος
    - Περίπτωση μη επιθυμητής λειτουργίας
    - Υπόδειξη διόρθωσης μοντέλου

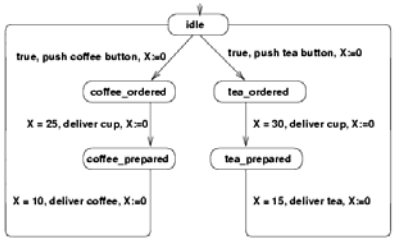
Model Checking

- Γενικευμένη αντιμετώπιση
  - Υλικό, λογισμικό, επικοινωνίες …
- Δυνατότητα μερικού ελέγχου
  - Των σημαντικότερων υποσυστημάτων
- Μειωμένη συμμετοχή χρήστη
- Κρισιμότητα ακρίβειας μοντέλου
  - Δυσκολία κατασκευής
  - Ταιριάζει σε εφαρμογές ελέγχου (όχι data intensive)
- Αυτόματη δημιουργία κώδικα
  - Κατευθείαν από το μοντέλο

Συμπεριλαμβάνοντας τον χρόνο

- Καταγωγή: Temporal logics
  - Χρήση αυτομάτων πεπερασμένων καταστάσεων
  - Έμμεση μόνο χρήση χρόνου (διάταξη συμβάντων)
- Προσθήκη της έννοιας του χρόνου
  - Real Time Temporal Logic
  - Metric Temporal Logic
  - Time Propositional Temporal Logic
  - Time Computational Tree Logic
  - Duration Calculus
  - …
- Διακριτή ή συνεχής αναπαράσταση χρόνου

Timed Automata



- ύπαρξη μεταβλητών clock
- συσχέτιση μεταβάσεων με
  - συνθήκη clock, ενέργεια, reset clock