ΕΠΛ664 – ΑΝΑΛΥΣΗ ΚΑΙ ΕΠΑΛΗΘΕΥΣΗ ΣΥΣΤΗΜΑΤΩΝ

Περιγραφή του μαθήματος

Στόχοι του μαθήματος

Αξιολόγηση

Βιβλιογραφία

Διδασκαλία

Διαλέξεις: Δευτέρα και Πέμπτη, 15:00 - 16:30

Φροντιστήριο /Εργαστήριο : 1½ ώρα εβδομαδιαίως

Ιστοσελίδα μαθήματος: http://www.cs.ucy.ac.cy/~annap/epl664/

Περιγραφή

Ανάλυση/Επαλήθευση συστημάτων αφορά στον έλεγχο κατά πόσο ένα σύστημα ικανοποιεί τις απαιτήσεις που υπάρχουν από αυτό.

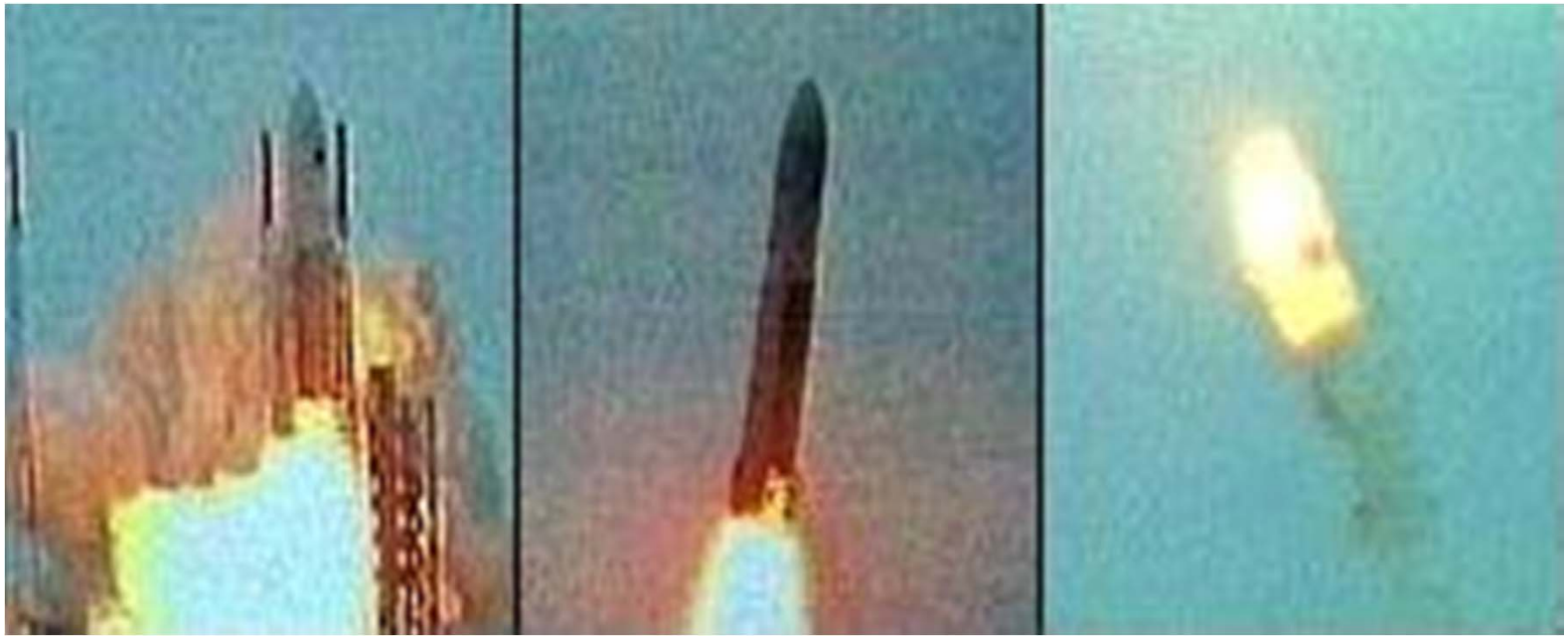
Περιγραφή

Ανάγκη για ανάλυση και επαλήθευση συστημάτων.

- Η κοινωνία της πληροφορίας είναι γεγονός. Υπολογιστές και προγράμματα έχουν εξαπλωθεί σε πολλαπλούς τομείς της ζωής μας:
  - ενθυλακωμένα συστήματα (embedded systems)
  - e-banking και e-shopping
  - μεταφορικά μέσα
  - ιατρική
  - …
- Η αξιοπιστία υλικού και λογισμικού είναι κύριας σημασίας
- Λάθη μπορεί να αποβούν όχι μόνο δαπανηρά (FDIV στο Pentium-II – 475 εκατομμύρια USD) αλλά και μοιραία (Therac-25)

"It is fair to state, that in this digital era correct systems for information processing are more valuable than gold."

Η τύχη του Ariane-5



Το Ariane-5 εκτοξεύθηκε στις 4 Ιουνίου 1996, για να συντριφθεί 36 δευτερόλεπτα αργότερα λόγω ενός σφάλματος στο λογισμικό ελέγχου.

(Το οποίο εκ των υστέρων εντοπίστηκε χρησιμοποιώντας τυπικές μεθόδους που θα μελετήσουμε στο μάθημα.)

Περιγραφή

- Θεωρία και πρακτική της Επαλήθευση και Ανάλυσης Συστημάτων βασισμένη σε *τυπικές μεθόδους* (formal methods).
- Τι είναι οι τυπικές μέθοδοι;
  - *"εφαρμοσμένα μαθηματικά" για τη μοντελοποίηση και ανάλυση υπολογιστικών συστημάτων*

Παρά του ότι βασίζονται σε μαθηματικά μπορούν να τύχουν χρήσης από οποιοδήποτε!

- Προσφέρουν
  - τη δυνατότητα της επαλήθευσης συστημάτων από τη φάση σχεδιασμού
  - αποδοτικές και αυστηρές μεθόδους ελέγχου συστημάτων (πιο μεγάλη κάλυψη και ψηλότερη εγγύηση ορθότητας)
  - μείωση του χρόνου/κόστους που απαιτείται για επαλήθευση
- Συστήνονται για δημιουργία λογισμικού κριτικής ασφάλειας από οργανισμούς όπως τους
  - ESA (European Space Agency), FAA (Federal Aviation Authority) και NASA.

Περιγραφή

"Formal methods should be part of the education of every computer scientist and software engineer, just as the appropriate branch of applied maths is a necessary part of the education of all other engineers."

NASA

Περιγραφή

Συγκεκριμένα το μάθημα θα μελετήσει:

- Πρότυπα μοντελοποίησης συστημάτων:
  - Συστήματα μεταβάσεων
  - Γραφικά πρότυπα
  - Άλγεβρες Διεργασιών
  - Αυτόματα
- Τεχνικές ανάλυσης συστημάτων:
  - Μοντελοέλεγχος (model-checking)
  - Ισοδυναμίες (simulations)
  - Εφαρμογή πειραμάτων (testing)
- Εργαλεία που επιτρέπουν την αυτοματοποιημένη ανάλυση συστημάτων:
  - SPIN
  - Concurrency WorkBench

Παράλληλα συστήματα, κατανεμημένα συστήματα, πρωτόκολλα επικοινωνίας, κλπ

Στόχοι του μαθήματος

- Εξοικείωση με διάφορες τεχνικές επαλήθευσης συστημάτων
- Αναγνώριση δυνατοτήτων και περιορισμών της κάθε μιας από αυτές
- Εξοικείωση με εργαλεία επαλήθευσης συστημάτων
- Διαδικασία: Επιλογή εργαλείου, μοντελοποίηση, ανάλυση, εύρεση λαθών
- Ειδικά θέματα: Χρόνος, πιθανότητα, ασφάλεια

Αξιολόγηση

5 σειρές ασκήσεων – 3 θεωρητικές – 2 πρακτικές	 3 × 5 = 15% 2 × 5 = 10%
Ενδιάμεση Εξέταση	25%
Τελική εξέταση	50%

Βιβλιογραφία

- D. Peled, *Software Reliability Methods*. Springer-Verlag, 2001.
- C. Baier and J.-P. Katoen, Principles of Model Checking. MIT Press, 2008.
- M. Huth and A. Ryan. *Logic in Computer Science: Modeling and Reasoning about Concurrent Systems.* Cambridge University Press, 2nd edition, 2004.
- L. Aceto, A. Ingólfsdóttír, K. G. Larsen and J. Srba, *Reactive Systems: Modelling, Specification and Verification*. Cambridge University Press, 2007.
- Επιλεγμένα άρθρα βιβλιογραφίας.