Software Engineering with Objects and Components

Massimo Felici
Course Organisation

- SEOC course webpage
  
  http://www.inf.ed.ac.uk/teaching/courses/seoc/

- Mailing List
  
  seoc-students@inf.ed.ac.uk

- Newsgroup
  
  eduni.inf.course.seoc1

- SEOC CVS repositories
Course Organisation

- Course Textbook
  

- Course Resources
  
  Lecture Notes and References

- Software
  
  Eclipse + UML plugin and Java
Course Organisation

- **Tutorials begin in week 3**
  
  Frequency: once a week
  
  Maximum 12 people per tutorial group

- **Coursework**
  
  in small teams (approx 3-4 people)
  
  two deliverables equally weighted
Course Organisation

- Coursework Deadlines
  
  1st deliverable: Friday, 30th October 2009
  
  2nd deliverable: Friday, 27th November 2009

- Assessment
  
  25% coursework; 75% degree examination
On Software Engineering

Massimo Felici
What is Software Engineering

Software Engineering is an engineering discipline that is concerned with all aspects of software production from the early stages of system specification to maintaining the system after it has gone into use.
Slide 1: What is Software Engineering

This lecture provides a very brief introduction to Software Engineering. The SEOC course focuses on engineering software systems using Objects and Components. The main learning objectives of the course involve the acquisition of software engineering knowledge and ability to design, assess and implement object-oriented systems. The course uses UML as modelling language. The course organisation embeds some general software engineering principles and practices.

Required Readings

Suggested Readings


Some Aspects of Software Engineering

- Software Processes
- Software Process Models
- Software Engineering Methods
- Costs
- Software Attributes
- Tools
- Professional and Ethical Responsibilities
Software Engineering is concerned with all aspects of software production. The main objective is to support software production in order to deliver software that is “fit for purpose”, e.g., good enough (functionally, non-functionally), meets constraints (e.g., time and financial) of the environment, law, ethics and work practices.

A Software Process is the set of activities and associated results (e.g., software specification, software development, software validation and software evolution) that produce a software product.

A Software Process Model is an overview of the software activities and results organisation.

Software Engineering processes (e.g., waterfall, spiral, etc.) arrange (deploy effort) activities differently. The SEOC organisation, to a certain extent, embeds some basic principles underlying different software engineering processes.
Essential software activities are:

- **Software Requirements**: gaining an accurate idea of what the users of the system want it to do.
- **Software Design**: the design of a system to meet the requirements.
- **Software Construction**: the realisation of the design as a program.
- **Software Testing**: the process of checking the code meets the design.
- **Software Configuration, Operation and Maintenance**: major cost in the lifetime of systems.

**Suggested Readings**

- Chapter 4 on Software Processes in Summerville’s book.
Why Software Fails?

- Complex causes (interactions) trigger software failures

- Software fails in context

- Some issues related to software engineering
  - Misunderstood requirements
  - Design issues
  - Mistakes in specification, design or implementation
  - Operational issues

- Faults, Errors and Failures
Slide 3: Why Software Fails?

Unfortunately, software still fails too often. Software fails in complex manners. Although the course stresses the importance of software designs and models, it is often difficult to understand how software engineering aspects (e.g., design, implementation, etc.) relate to or address software failures. Software failures may have dependability (e.g., safety, reliability, etc.) as well as financial implications.

Required Readings


Suggested Readings

• Chapter 3 on Critical Systems in Sommerville’s book.
Faults, Errors and Failures

- **Fault** - The adjudged or hypothesized cause of an error is called a fault. A fault is active when it causes an error, otherwise it is dormant.

- **Error** - The deviation from a correct service state is called an error. An error is the part of the total state of the system that may lead to its subsequent service failure.

- **Failure** - A failure is an event that occurs when the delivered service deviates from correct service.

*Warnings: different understandings of faults, errors and failures.*
An important aspect is to understand how faults, errors and failures relate each other. Research and practice in engineering safety-critical systems emphasize the underlying mechanisms of software failures. Note that understanding these concepts (i.e., faults, errors and failures) in practice often requires expertise within specific application domains, which might have different interpretations of them.

Suggested Readings

Some “Famous” Software Failures

• Patriot Missile failure
  – Inaccurate calculation of the time since boot due to computer arithmetic errors
  – Coding errors may effect overall software system behaviour

• The Ariane 5 Launcher failure
  – The complete loss of guidance and altitude information 37 seconds after start of the main engine ignition sequence
  – The loss of information was due to specification and design errors in the software of the inertial reference system
  – The software that failed was reused from the Ariane 4 launch vehicle. The computation that resulted in overflow was not used by Ariane 5
Some “Famous” Software Failures

- The London Ambulance fiasco

- Therac 25 and other medical device failures
  - (Software) Reliability is different than (System) Safety
Slide 6: Some “Famous” Software Failures

Required Readings


Suggested Readings


The Patriot Missile Failure

**Accident Scenario:** On February 25, 1991, during the Gulf War, an American Patriot Missile battery in Dharan, Saudi Arabia, failed to track and intercept an incoming Iraqi Scud missile. The Scud struck an American Army barracks, killing 28 soldiers and injuring around 100 other people.
Slide 7: The Patriot Missile Failure

The Patriot Missile Failure

- **Fault** - Inaccurate calculation of the time since boot due to computer arithmetic errors.

- **Error** - The small chopping error, when multiplied by the large number giving the time in tenths of a second, lead to a significant error of 0.34 seconds.

- **Failure** - A Scud travels at about 1,676 meters per second, and so travels more than 500 meters in this time. This was far enough that the incoming Scud was outside the range gate that the Patriot tracked.
Slide 8: The Patriot Missile Failure

**Fault** - The time in tenths of second as measured by the system’s internal clock was multiplied by 1/10 to produce the time in seconds. This calculation was performed using a 24 bit fixed point register. In particular, the value 1/10, which has a non-terminating binary expansion, was chopped at 24 bits after the radix point.
**Slide 8: The Patriot Missile Failure**

**Error** - Indeed, the Patriot battery had been up around 100 hours, and an easy calculation shows that the resulting time error due to the magnified chopping error was about 0.34 seconds. The binary expansion of 1/10 is

$0.0001100110011001100110011001100...$

The 24 bit register in the Patriot stored instead

$0.00011001100110011001100$

introducing an error of

$0.0000000000000000000000011001100...$ binary, or about $0.000000095$ decimal. Multiplying by the number of tenths of a second in 100 hours gives

$0.000000095 \times 100 \times 60 \times 60 \times 10 = 0.34$.

Ironically, the fact that the bad time calculation had been improved in some parts of the code, but not all, contributed to the problem, since it meant that the inaccuracies did not cancel.
The Patriot Missile Failure

- Identifying coding errors is very hard
  seemingly insignificant errors result in major changes in behaviour

- Original fix suggested a change in procedures
  reboot every 30 hours impractical in operation

- Patriot is atypical
  coding bugs rarely cause accidents alone

- Maintenance failure failure of coding standards and traceability
Supporting Software Engineering Practices

• Provides a range of graphical notations that capture various aspects of the engineering process

• Provides a common notation for various different facets of systems

• Provides the basis for a range of consistency checks, validation and verification procedures

• Provides a common set of languages and notations that are the basis for creating tools
Required Readings  UML course textbook

• Chapter 1 on the Introduction to the Case Studies.

• Chapter 2 on the Background to UML.
Some UML Diagrams

- Use Case Diagrams
- Class Diagrams
- Interaction Diagrams
  - Sequence and Communication Diagrams
- Activity Diagrams
- State Machines
Slide 11: Some UML Diagrams

- Use Case Diagrams
  Used to support requirements capture and analysis; show the actors involvement in system activities

- Class Diagrams
  Capture the static structure of systems; associations between classes

- Interaction Diagrams
  Capture how objects interact to achieve a goal
Slide 11: Some UML Diagrams

- Activity Diagrams
  
  Capture the workflow in a situation

- State Machines:
  
  Capture state change in objects of the system

- Other Diagrams: Component and Deployment Diagrams
Required Readings

• UML course textbook
  – Chapter 1 on the Introduction to the Case Studies.
  – Chapter 2 on the Background to UML


Suggested Readings

  - Chapter 1 for a general account of Software Engineering
  - Chapter 3 on Critical Systems
  - Chapter 4 on Software Processes
Summary

• SEOC organisation

• An introduction to Software Engineering

• Why Software Fails

• Faults, Errors and Failures

• Examples of Software Failures

• An Outline of some UML diagrams

• Required Readings and Suggested Readings