Phd course on

Formal modelling and analysis of interactive systems

Part 1
Introduction

Course Motivations and Structure, Terminology, Human Errors

Antonio Cerone

United Nations University

International Institute for Software Technology

Macau SAR China

email: antonio@iist.unu.edu

web: www.iist.unu.edu

Contents

Motivations

Motivation — Example

This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
[...]
The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box [...]

Example: good design?

This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
[...]
The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box [...]

Example: but ...

This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
[...]
The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box [...]

Example: catastrophe!

> This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
> [...]
> The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box — it was only as we hit the 'Confirm' button that we noticed the word 'delete' at the top...

[Dix et al. 98]

Alan Dix, Janet Finaly, Gregory Abowd, Russel Beale.

Human-Computer Interaction.

Prentice Hall, 2nd Edition, 1998.

Example: design problems?

> This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
> [...]
> The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box — it was only as we hit the 'Confirm' button that we noticed the word 'delete' at the top...

Design logic takes an ideal user into account

Problem: real user $\neq$ ideal user imagined by the designer

Example: poor usability!

> This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
> [...]
> The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box — it was only as we hit the 'Confirm' button that we noticed the word 'delete' at the top...

Design logic does not address user's capabilities and limitations

Why Poor Usability

- User friendly and easy to use from the point of view of the designer
- the designer is potentially a user $\Longrightarrow$
  - implicit assumptions on the user's capabilities and behaviour
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

User neglected $\Longrightarrow$

- User friendly and easy to use from the point of view of the designer
- the designer is potentially a user $\Longrightarrow$
  - implicit assumptions on the user's capabilities and behaviour
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

User-centered Design

- USER = first priority in the requirements of interactive systems (SE)
- the designer is potentially a user $\Longrightarrow$
  - implicit assumptions on the user's capabilities and behaviour
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

Implicit Assumptions $\Longrightarrow$

- USER = first priority in the requirements of interactive systems (SE)
- the designer is potentially a user $\Longrightarrow$
  - implicit assumptions on the user's capabilities and behaviour
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

Study of Human Being

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

Positive Assumptions $\Longrightarrow$

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
  - explicit assumptions on the user's knowledge of the system — the user has entirely read and understood the manual
- interface viewed as plug-in separate from the rest of the system

Negative Assumptions

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
- explicit assumptions on user's physical and cognitive limitations and environmental and social constraints (Ergonomics, Cognitive Science and Sociology)
- interface viewed as plug-in separate from the rest of the system

Separate HCI Design $\Longrightarrow$

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
- explicit assumptions on user's physical and cognitive limitations and environmental and social constraints (Ergonomics, Cognitive Science and Sociology)
- interface viewed as plug-in separate from the rest of the system

Integrated HCI Design

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
- explicit assumptions on user's physical and cognitive limitations and environmental and social constraints (Ergonomics, Cognitive Science and Sociology)
- interface developed integrally with the rest of the system (SE) to support tasks people want to do and forgive careless mistakes

Improving Usability

- USER = first priority in the requirements of interactive systems (SE)
- study of the mind (perception, thinking and learning) and behaviour of the human being (Psychology) and related experiments
- explicit assumptions on user's physical and cognitive limitations and environmental and social constraints (Ergonomics, Cognitive Science and Sociology)
- interface developed integrally with the rest of the system (SE) to support tasks people want to do and forgive careless mistakes

HCI — Human-computer Interaction

Multidisciplinary Approach

Contribution from many disciplines:

- Software Engineering
- Psychology (Social, Cognitive, Personality, Industrial and Engineering Psychology)
- Ergonomics
- Cognitive Science
- Sociology

Wide Range of Expertise

- Psychology and Cognitive Science to give knowledge of the user's perceptual, cognitive and problem-solving skills
- Ergonomics for the user's physical capabilities
- Sociology to help understandig the wider context of the interaction
- Computer Science and Software Engineering to be able to build the necessary technology
- Business to be able to market the built technology
- Graphic Design to produce an effective interface presentation
- Technical Writing to produce the manuals

Too much expertise to be included in a design team

In practice people tend to take a strong stance on one side or another

Interdisciplinary Research

Multidisciplinary Research Centres:

- UCL Interaction Centre
  (University College London, London, UK)
  http://www.uclic.ucl.ac.uk/
- Key Centre for Human Factors and Applied Cognitive Psychology
  (University of Queensland, Brisbane, Australia)
  http://www.humanfactors.uq.edu.au/
- NASA Human Systems Integration Division
  (NASA Ames Research Centre, USA)
  http://hsi.arc.nasa.gov/
  - HCI Group: http://hci.arc.nasa.gov/

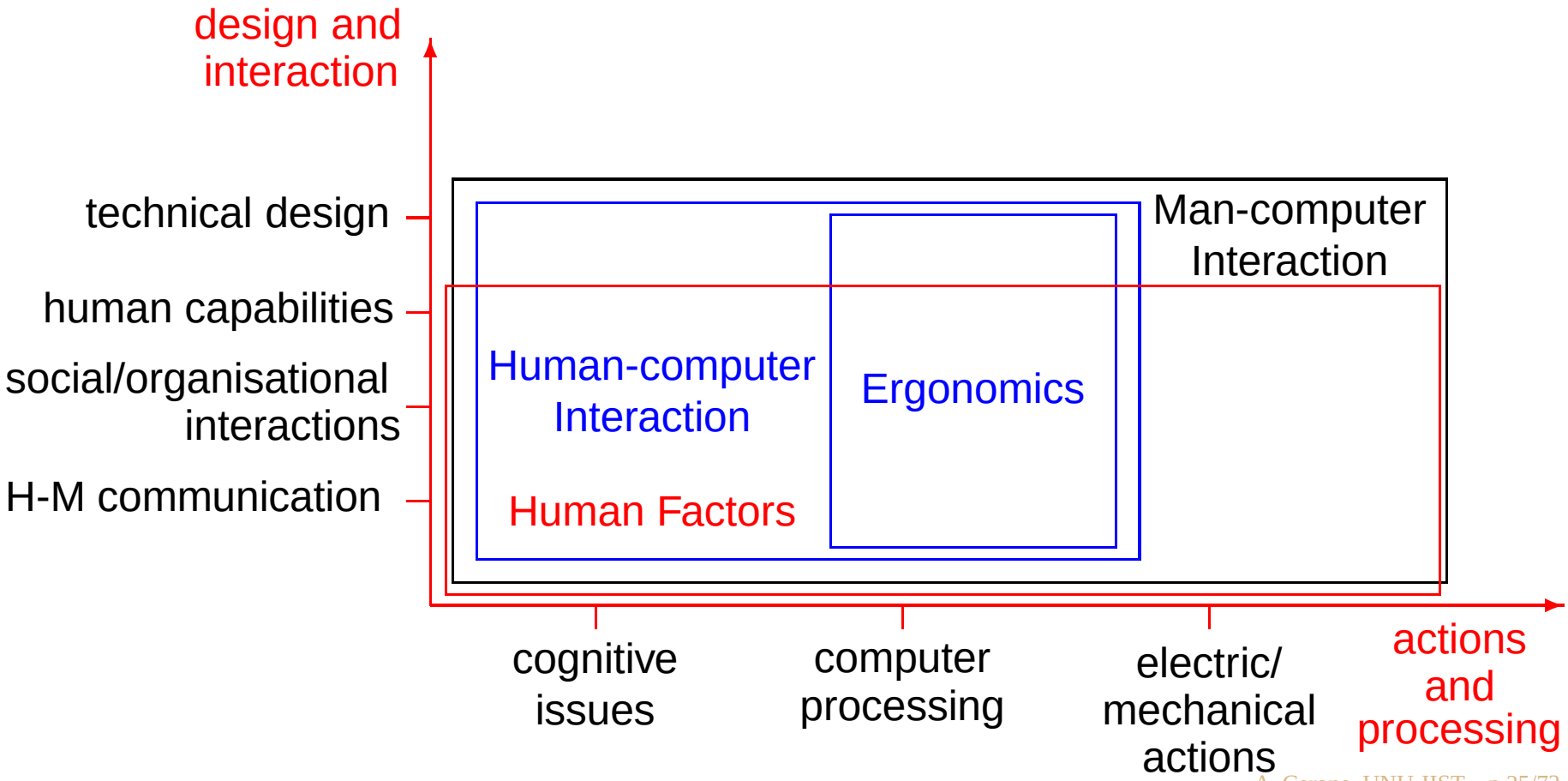
Synonyms?

- Human-computer Interaction (Computer-human Interaction)
- Man-machine Interaction
- Industrial Engineering
- Engineering Psychology
- Human Factors
- Ergonomics

Some Differences

Traditionally: Ergonomics preferred term in the UK

Human Factors preferred term in the US



History of HCI

- study of human performance
  early 20th century in factories
  emphasis on manual tasks
- 2nd World War
  urged study of interaction human-machine
  goal: produce more powerful weapons
- 1949
  Ergonomic Research Society
- 1982
  Conference on Human Factors in Computing, Gaithersburg
  HCI as a professional community

Def of HCI (ACM)

the discipline concerned with the design, evaluation, and implementation of interactive computing systems for human use and with the study of major phenomena surrounding them

[ACM special interest Group on Computer-Human Interaction Curriculum Development Group, 1992]

Def of HCI (others)

the study of interaction between people (users) and computers

[Wikipedia] (accessed in 2010)

the study of people, computer technology and the ways these influence each other

[Dix et al. 98]

Human Error

Requirements and Goal of HCI

the study of people, computer technology and the ways these influence each other

[Dix et al. 98]

Requirements of HCI

- computer technology
- the people who interact with it

Goal of HCI

- usability $\Longrightarrow$ to prevent user errors

Consequences of Human Errors

may just be temporary inconvenience or annoyance in interactive systems such as

- word processors
- VCR, DVD
- radio, CD, AC in cars?

distract the driver
$\Longrightarrow$ may cause human errors in driving
$\Longrightarrow$ it's unsafe!!!

Catastrophic Effects

Human errors may cause

- safety violations in domains such as chemical and nuclear plants, air traffic control, trasporation systems, health systems
- security violations in domains such as e-commerce, e-voting, defence

with catastrophic effects
$\Longrightarrow$ need to use formal methods

National Standards

used to deal with safety and security issues without mentioning HCI aspects

$\Longrightarrow$ human error appears in many accident reports as the main cause of the catastrophe

Recently national health and safety standards are starting to explicitly include usability

Example
EC directive 90/270/EEC

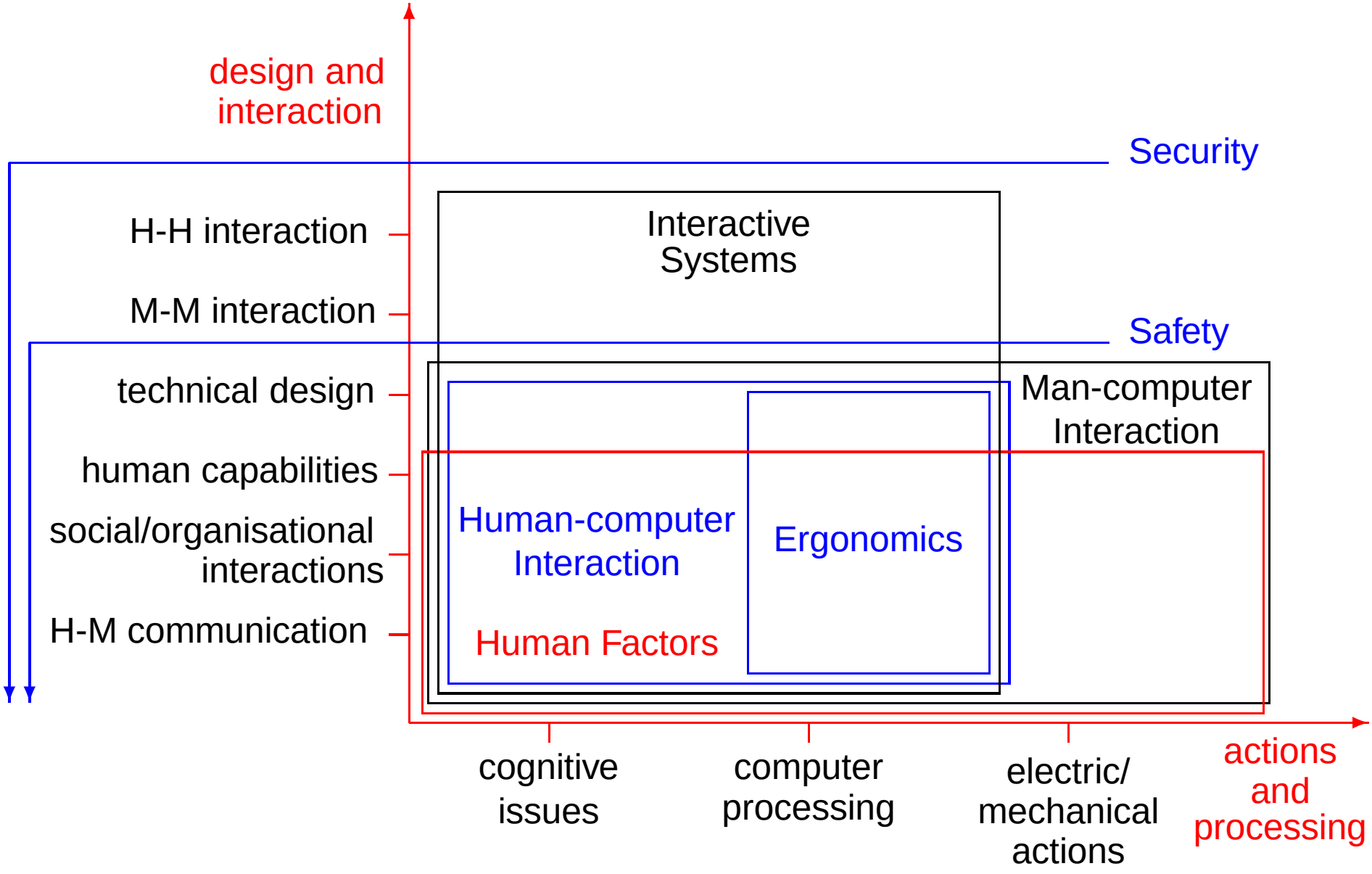
EC directive 90/270/EEC

http://osha.europa.eu/data/legislation/5

incorporated into member countries legislations
requires employers to ensure that software

- is suitable for the task
- is easy to use and adaptable to the user's knowledge and experience
- provides feedback on performance
- displays information in a format and at a pace that is adapted to the user
- conforms to the *principles of software ergonimics*

Interactive Systems



Interactive Systems Perpective

- user — an individual user, a group of users, a sequence of users
- computer/machine — any computer technology, a process control system, an embedded system
  including non-computerised and human parts
- interactions
  - human-machine
  - machine-machine
  - human-human

  which may be direct or indirect

Goal of HCI

increase usability

$\Longrightarrow$ to prevent user errors

or at least
$\Longrightarrow$ without increasing likelihood or severity of user errors, which may lead to

- system failure
- catastrophic consequences

User Errors

> This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.
> [...]
> The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box — it was only as we hit the 'Confirm' button that we noticed the word 'delete' at the top...

Design choices aimed to increase usability,

- increased likelihood and severity of errors
- with catastrophic consequences

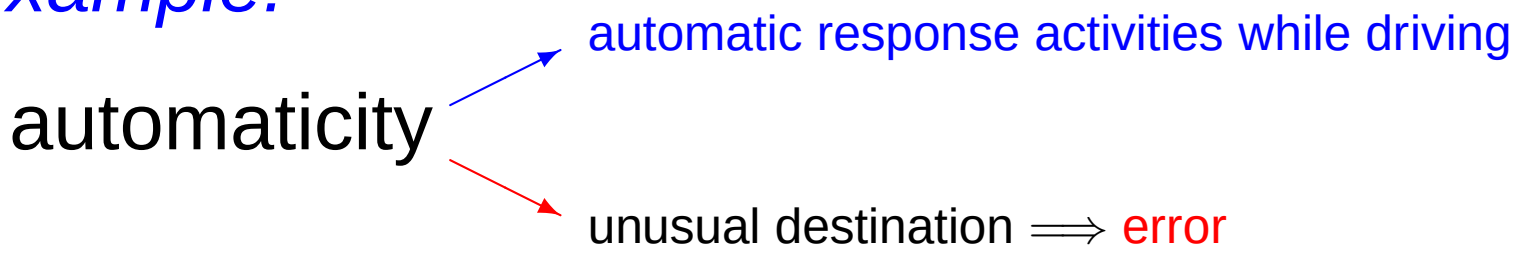
Nature of Errors

Correct performance and systematic errors are two sides of the same coin.

[Reason 90, page 2]

The same processes that govern correct human perception, thought, action and feeling are also responsible for human errors

Example:



Vision

- Highly complex activity with a range of physical and perceptual limitations
- Primary source of information for the average person
- Two stages of visual perception
  - physical reception of stimulus from outside world
  - processing and interpretation of the stimulus
    (construction from incomplete information)

Vision: Size and Depth

- visual angle gives a global perception of size and distance, which needs interpretation:
  - law of size constancy the size of an object is perceived as constant when it moves away from the observer
  - cues help perceiveing depth: overlapping objects, other objects in the field of view, familiarity, ...
- visual acuity limits detail perception of
  - single lines to 0.5 seconds
  - spaces between lines to 30 seconds

Context Resolves Ambiguity

$$13$$

$$2\ 3\ 5\ 7\ 11\ 13\ 17\ 19\ 23$$

$$A\ 13\ C$$

$$\alpha\ 13\ \gamma$$

Illusions

Compensation and ability to solve ambiguities may create illusions:

- Which line is longer?
  Muller-Lyer illusion and Ponzo illusion
- Proof-reading illusion

Muller-Lyer Illusion

Which line is longer?

Ponzo Illusion

Which line is longer?

Proof-reading Illusion

Was the text correct?

Definitions: Error

All those occasions in which a planned sequences of mental or physical activities fails to achieve its intended outcome and when these failures cannot be attributed to the interventon of some chance agency

[Reason 90, page 9]

Definitions: Slips and Lapses

Slips and lapses result from some failures in the execution and/or storage stage of an action sequence, regardless of whether or not the plan which guided them was adequate to achieve its objective

[Reason 90, page 9]

Two types of errors:

execution failure and memory failure

Definitions: Slips

> Slips and lapses result from some failures in the execution and/or storage stage of an action sequence, regardless of whether or not the plan which guided them was adequate to achieve its objective
>
> [Reason 90, page 9]

Slips (execution failure) are potentially observable as externalised actions-non-as-planned

- slips of the tongue
- slips of the pen
- slips of action

Definitions: Lapses

> Slips and lapses result from some failures in the execution and/or storage stage of an action sequence, regardless of whether or not the plan which guided them was adequate to achieve its objective
>
> [Reason 90, page 9]

Lapses (memory failure) are more covered error forms, largely involving failures of memory, that do not necessarily manifest themselves in actual behaviour and may only be apparent to the person who experiences them

Definitions: Mistakes

All deficiencies and failure in the in the judgemental and/or inferential processes involved in the selection of an objective or in the specification of the means to achieve it, irrespective of whether or not the actions directed by this decision-scheme run according to plan

[Reason 90, page 9]

- planning failure
- more subtle, complex and less understood
- often they constitute a far greater danger
- harder to detect

Example: Errors

This is the authors' second attempt at writing this introduction. Our first attempt fell victim to a design quirk coupled with an innocent, though weary and less than attentive, user.

[...]

The 'save' and 'delete' options, both of which are correctly classified as file-level operations, are consequently adjacent items in the menu. [...] it is all too easy for the hand to slip, inadvertently selecting delete instead of save. Of course, the delete option, being well thought out, pops up a confirmation box allowing the user to cancel a mistaken command. Unfortunately, the save option produces a very similar confirmation box — it was only as we hit the 'Confirm' button that we noticed the word 'delete' at the top...

What types of errors Two slips

Error Recoverability

Ability to reach a desired goal after recognition of some error in previous interaction

Recoverability Directions

Ability to reach a desired goal after recognition of some error in previous interaction

Recovery directions

- backward recovery attempt to undo the effect of previous interaction in order to return to a previous state (confirm box, undo menu option, U-turn while driving)
- forward recovery acceptance of the current state and negotiation from that state toward the desired state (retyping what is lost, altenative route while driving)

Recoverability is linked to Reachability

Recoverability Initiator

Ability to reach a desired goal after recognition of some error in previous interaction

- initiated by the system connected to fault-tolerance, safety, reliability, dependability
- initiated by the user determinates user's intent towards forward or backward recoverability

Commensurate Effort

Principle of Commensurate Effort

If it is difficult to undo a given effect on the state, then it should be difficult to do it in the first place.

Conversely, easily undone action should be easily doable

Error Predictability

Degree of Predictability

- low for variable errors
- high for constant errors

Accuracy of error prediction depends on the extent to which factors giving rise to the error are understood

Error predictions forcast

- conditions under which errors occur
- forms taken by errors

Most error predictions are qualitative or probabilistic

Classification of Errors

Three levels of classification

- behavioural: observable features of the erroneous behaviour (fenotype errors)
- contextual: triggering factors and underlying error tendencies (facilitating causes rather than actual error explanations)
- conceptual: based on assumptions about cognitive mechanisms involved in error production (genotype errors)

Course

Goals of the Course

Enable students

- to understand how human behaviour and human error may affect system correctness
- to use formal methods
  - for modelling
    - computer/machine
    - user's tasks (observable behaviour)
    - user's cognitive aspects
  - for verifying properties of
    - interactive systems
    - cognitive theories

Course Philosophy

- concepts introduced through examples:
  - Automatic Teller Machine (ATM)
  - Air Traffic Control system (ATC)
  - Groupware System (GWS)
- everything hands-on

Structure of the Course

1. Introduction
2. Formal Tools and HCI Concepts (ATM)
3. Formal Analysis and Cognitive Models (ATM)
4. Tasks and Task Failures (ATC)
5. Usability and Security (GWS)
6. Quantitive Aspects and Cognitive Architectures (if we have time)

Examinations

- Seminar (45 minutes + questions) during 27-30 December 2010 on topic and papers suggested by the lecturer or proposed by the student
- Written Report on topic suggested by the lecturer or proposed by the student
  Deadline: 31 March 2011
- Short Written Report and Code Development on topic suggested by the lecturer or proposed by the student
  Deadline: 31 March 2011

Schedule

1. Thursday 9 December 2010, 9:00-12:00
2. Tuesday 14 December 2010, 9:30-12:30
3. Wednesday 15 December 2010, 9:30-12:30
4. Thursday 16 December 2010, 9:30-12:30
5. Tuesday 21 December 2010, 9:30-12:30
6. Wednesday 22 December 2010, 9:30-11:30

Online Materials

Course website
http://www.di.unipi.it/ cerone/courses/fmais-2010/,
which contains:

- slides
- code
- papers

References

[Dix et al. 98]

Alan Dix, Janet Finaly, Gregory Abowd, Russel Beale.
Human-Computer Interaction.
Prentice Hall, 2nd Edition, 1998.

HCI Textbook

One of the most complete general textbooks in HCI, also introduces the use of seveal formal notations, such as Petri nets, CSP, temporal logic, Z. There is now a 3rd edition.
Complementary materials available online at

http://www.hiraeth.com/books/hci/

[Preece et al. 94]

Jenny Preece, Yvonne Rogers, Helen Sharp, David Benyon, Simon Holland and Tom Carey. *Human-Computer Interaction*. Addison Wesley, 1994.

HCI Textbook

The first HCI textbook to contain all pedagogical features (examples, exercises, etc.). Now a bit old. Book review available online at

http://www.acm.org/∼perlman/preece.html

[Dix 91]

Alan Dix.
Formal Methods for Interactive Systems.
Academic Press, 1991.

FMIS Textbook
Out of print, but available online at
http://www.hiraeth.com/books/formal/

[Reason 90]

James Reason.
Human Error.
Cambridge University Press, 1990.

[FMIS 06]

A. Cerone and P. Curzon.
Proceedings of FMIS 2006.
ENTCS 183, Elsevier, 2007

Extended version of a selection of the papers has been published in
Software and System Modeling Vol. 4, No. 2, Springer, 2008

[FMIS 07]

A. Cerone and P. Curzon.
Proceedings of FMIS 2007.
ENTCS , Elsevier, 2007

Extended version of a selection of the papers has been published in
Formal Aspects of Computing Vol. 21, No. 6, Springer, 2009

[FMIS 09]

M. Harrison and M. Massink.
Proceedings of FMIS 2009.
EPTCS, 2009