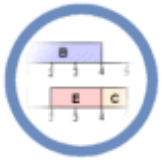




Lecture 11
Introduction to Reliability (Part 1)

<lecturer, date>

Outline

- Introduction to dependability
- Introduction to reliability
- Examples
- Reliability issues
- Means to achieve reliability

Introduction to dependability

- Definition: "*The ability of a computer system to deliver service that can justifiably be trusted.*"

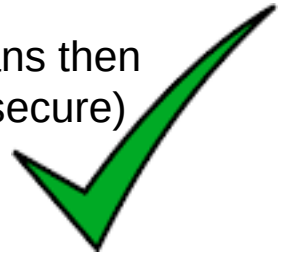
- Example 1: consider the airbag system widely deployed in cars

  – The air bag should inflate in the event of a car crash
  – If the airbag does not inflate **always** whenever there is a crash, it cannot be termed as dependable.

- Example 2: consider Bob who has an email account

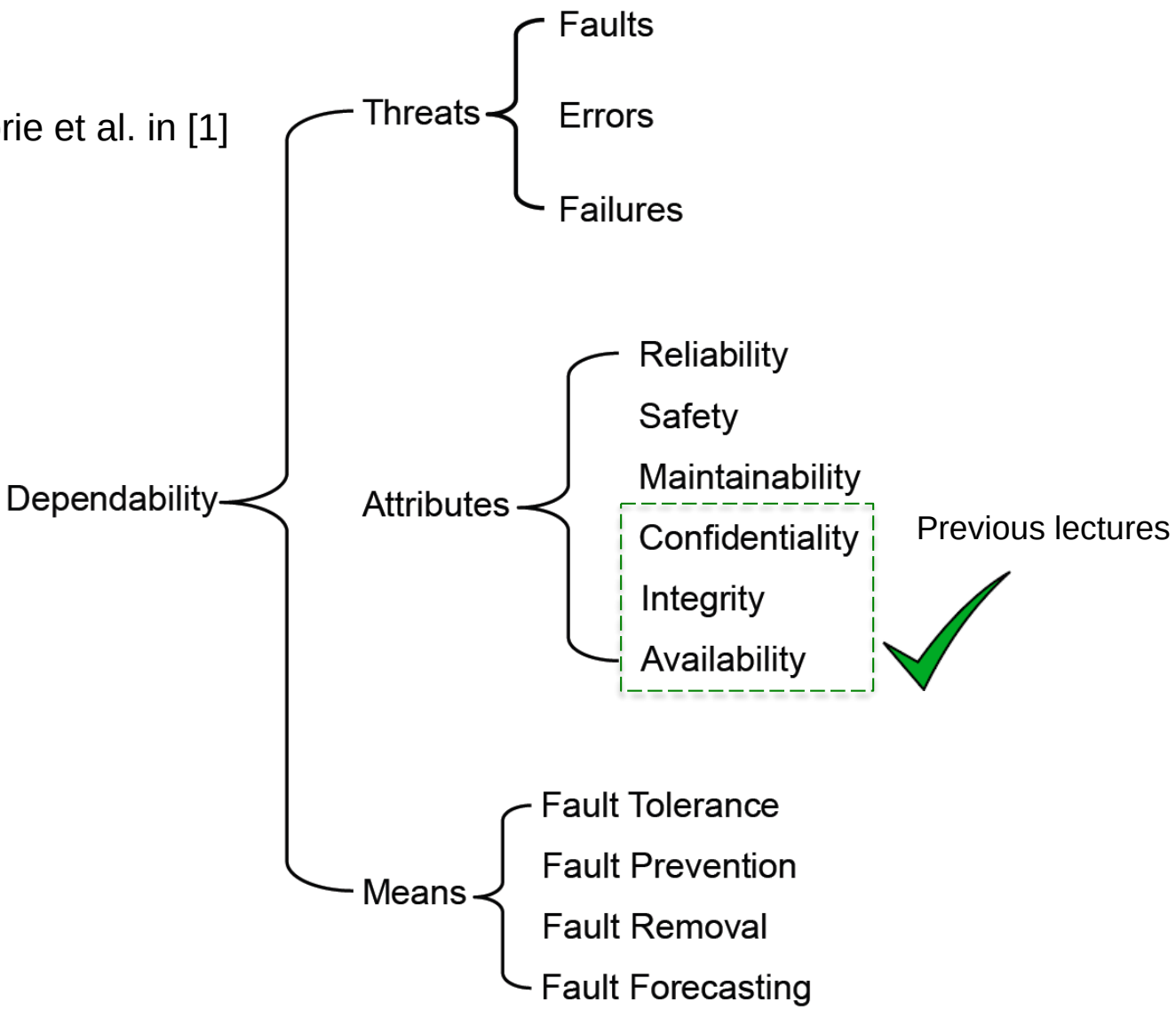
Already seen

  - Only Bob should be able to read his email
  – If Alice is able to gain access to Bob's email using some malicious means then the email system cannot be termed as dependable (or more precisely secure)



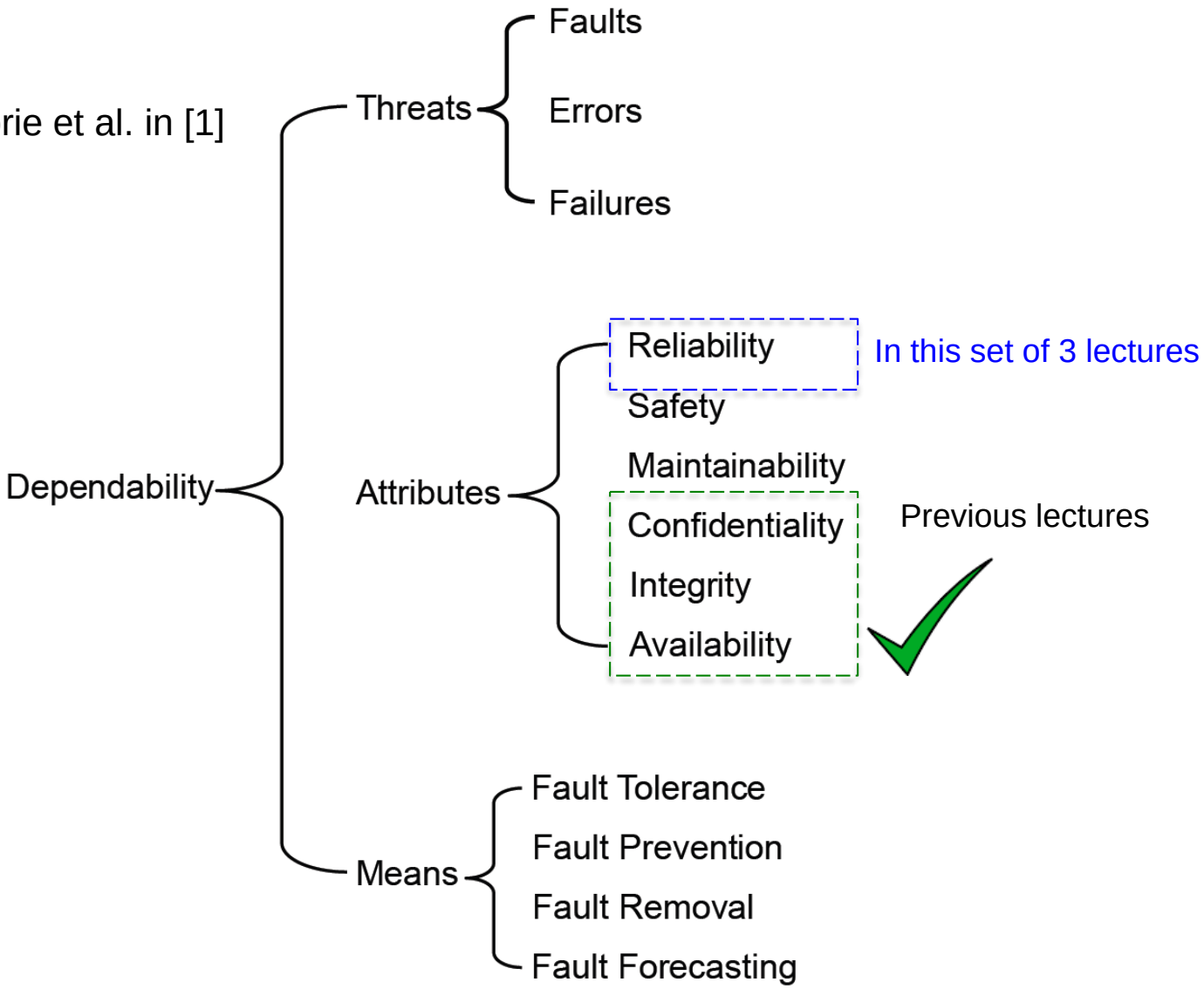
The dependability tree

Presented by Laprie et al. in [1]



The dependability tree

Presented by Laprie et al. in [1]



Introduction to dependability

- Definition: "*The ability of a computer system to deliver service that can justifiably be trusted.*"

- Example 1: consider the airbag system widely deployed in cars

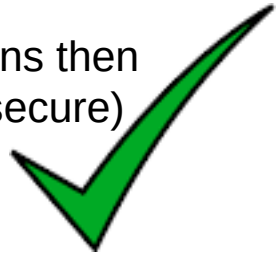
Reliability Issue

The air bag should inflate in the event of a car crash

  - If the airbag does not inflate **always** whenever there is a crash, it cannot be termed as dependable.

- Example 2: consider Bob who has an email account

  - Only Bob should be able to read his email
  - If Alice is able to gain access to Bob's email using some malicious means then the email system cannot be termed as dependable (or more precisely secure)



Outline

- Introduction to dependability
- Introduction to reliability
- Examples
- Reliability issues
- Means to achieve reliability

Introduction to reliability

- Definition: "*The probability that a computer system delivers a service that can justifiably be trusted.*"
- Faults in the system give rise to errors which eventually leads to a failure affecting the reliability
- Fault tolerance strategies, most commonly in the form of redundancy, are employed to tolerate faults
- Fault tolerance typically imply increased Size, Weight and Power (SWaP) requirements that is critical for mobile applications

Outline

- Introduction to dependability
- Introduction to reliability
- Examples
- Reliability issues
- Means to achieve reliability

Mishaps- Ariane 5

Self-destructed 37 sec after launch

Cause(s)

- buffer overflow: data conversion from 64-bit floating point to 16-bit signed integer
- software reuse (from Ariane 4)

Results

- one of the most expensive computer bugs in history
- 10 years of development and > $7 billion

Mishaps- Patriot Missile bug

February 1991 – A Scud missile is not intercepted by the Patriot battery – hits a soldier tent and kills 28 American soldiers

- Main cause – a bug in the clock of the control unit, which resulted in erroneous position prediction by 600 meters

- Originally designed to intercept Soviet missiles (travelling at MACH 2) running for short periods of time

- Reused during “Desert Storm” against Scud missiles (travelling at MACH 5), running for long periods of time

- Accumulation of clock delays lead to incorrect calculation of the trajectory

Mishaps- Turkish Airlines

February 2009– A Turkish airlines flight crashed in Schipol-Amsterdam airport.

- Altimeter hardware was faulty
- Caused incorrect altimeter output
- The autopilot decreased the power to the engine too early

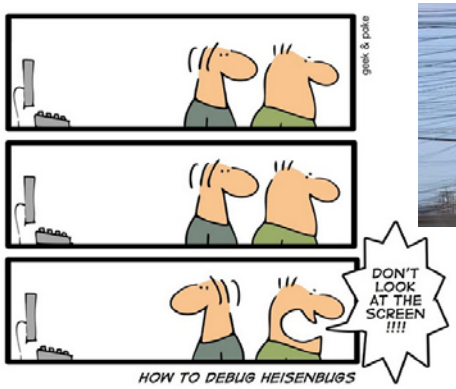
Outline

- Introduction to dependability
- Introduction to reliability
- Examples
- Reliability issues
- Means to achieve reliability

What can go wrong?

- Permanent hardware faults
  - Wiring, connectors, processors, sensors, actuators

- Transient & intermittent faults
  - Electromagnetic interference (EMI) (both internal and external), hesienbugs



Outline

- Introduction to dependability
- Introduction to reliability
- Examples
- Reliability issues
- Means to achieve reliability

What to do about faults?

- Fault tolerance
  - to cope with the effects of faults
  - typically by redundancy
- Verification and validation
  - to identify and eliminate faults
- Safety analysis
  - to focus on the most important faults

What to do about faults?

- Fault tolerance
  - to cope with the effects of faults
  - typically by redundancy

Lecture 12

- Verification and validation
  - to identify and eliminate faults

- Safety analysis
  - to focus on the most important faults

What to do about faults?

- Fault tolerance
  - to cope with the effects of faults
  - typically by redundancy

Lecture 12

- Verification and validation
  - to identify and eliminate faults

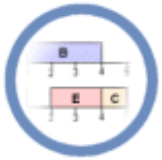
Lecture 13

- Safety analysis
  - to focus on the most important faults

References

1) Basic concepts and taxonomy of dependable and secure computing, Avizienis, A. ; Laprie, J.-C. ; Randell, B. ; Landwehr, C., IEEE Transactions on Dependable and Secure Computing, 2004
2) What really happened on Mars? http://research.microsoft.com/en-us/um/people/mbj/Mars_Pathfinder/Mars_Pathfinder.html
3) J. Gleick, A bug and a crash, http://www.around.com/ariane.html





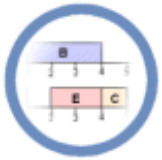
Lab 11
Introduction to Reliability (Part 1)

<lecturer, date>

Description

- How will your app behave in case of faults?
  - Develop mechanisms to introduce or simulate faults in the app
    - modify the app such that it sends wrong values for temperature and pressure randomly
  - Develop mechanisms to introduce or simulate faults in the water tank controller
    - modify the water tank controller such that it drops received values for temperature and pressure randomly
  - Draw a graph that plots the expected temperature and pressure of the water tank controller vs. the actual temperature and pressure for *30* simulations
  - Write a report that details your conclusions and reflections





Seminar 11
Introduction to Reliability (Part 1)

<lecturer, date>

Description

1. Read the following articles and write a short summary along with your reflections.

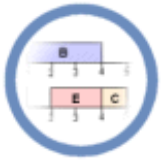
2. Discuss the articles in class.

N. G. Leveson, “High-pressure steam engines and computer software,” in Proceedings of the 14th International Conference on Software Engineering, 1992, http://sunnyday.mit.edu/steam.pdf

What really happened on Mars? http://research.microsoft.com/en-us/um/people/mbj/Mars_Pathfinder/Mars_Pathfinder.html

N. G. Leveson, The role of software in spacecraft accidents, http://sunnyday.mit.edu/papers/jsr.pdf





Mini-project 11
Introduction to Reliability (Part 1)

<lecturer, date>

Description

- Submit a report summarizing the articles and the discussions during the seminar.
- The report should also include your reflections on the reliability aspects of mobile applications that control embedded systems.