DCML-CPS - Module 1

Basics and Metrology

Tommaso Zoppi
University of Trento – Povo (TN - Italy)
tommaso.zoppi@unitn.it
tommaso.zoppi@unifi.it

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Data Collection and Machine Learning for Critical Cyber-Physical Systems

- First Semester - 6 ETCS

Dott. Tommaso Zoppi (4 ETCS)

Dipartimento di Matematica e Informatica, Università di Firenze

tommaso.zoppi@unifi.it http://rcl.dimai.unifi.it

Prof. Andrea Ceccarelli (2 ETCS)

Dipartimento di Matematica e Informatica, Università di Firenze

andrea.ceccarelli@unifi.it http://rcl.dimai.unifi.it

RCL
RESILIENT COMPUTING LAB

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Why DCML-CPS (DCML)?

Everybody wants to understand if their system is behaving correctly

- To detect errors, intrusions, anomalies and take countermeasures before failures happen
- Nice in theory, but how can I do it in practice?
- Downloading antiviruses? OK but covers only part of the problem

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Why DCML-CPS (DCML)?

Everybody wants to understand if their system is behaving correctly

- Thus, I have to
- understand how to monitor my system (DCML)
- know how to take advantage of monitored data (DCML)
  - Overall, a course that teaches very important concepts but also has practical implications and prepares the student for tasks that are usually critical in companies

Exam

- Project, + oral interview if students ask it

- Ideally, the project will be developed throughout the course
  - Aside from the first 2-3 lectures, the course will present a theoretical concept, and then we will try it, building the project step by step

- The project will end up with the development of an anomaly detector for your laptop

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Course Map

1. Basics of Metrology
2. Monitoring

Monitoring

Testing

3. Fault Injection
4. Robustness Testing

5. Data Analysis
6. Supervised ML
7. Unsupervised ML
8. Meta-Learning
9. Error/Intrusion Detection

Anomaly Detection

Tools & Libs

Course Map

12. DNNs & Libs
13. Robust Image Processing
14. Adversarial Attacks and Defenses
15. Embedded Networks

Deep Learning

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Course Map

1. Basics and Metrology
2. Monitoring

Monitoring

Testing

3. Fault Injection
4. Robustness Testing

5. Data Analysis
6. Supervised ML
7. Unsupervised ML
8. Meta-Learning
9. Error/Intrusion Detection

Anomaly Detection

Tools & Libs

Deep Learning

Basics and Dependability

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Quantitative Analysis of Systems

- What is the meaning of Quantitative Analysis???
  - Quantitative Analysis often has validation purposes, but…
- What is Validation?
  - What is Validated/Measured?
    - Dependability, but…
- What is the meaning of Dependability?

System

- A system can be considered a collection of
  - hardware
  - networks
  - operating systems, and
  - application software
- that is intended to be dependable, secure, survivable or have predictable performance.

Validation

- **Specification** - A description of what a system is supposed to do.
- **Realization** - A description of what a system is and does.

Validation - the process of determining whether a realization meets its specification.

Validation vs Verification

- Validation is different from Verification!

Verification is a process of determining if the system/software is designed and developed as per the specified requirements.

Validation (we know) is the process of checking if the system/software (end product) has met the client's true needs and expectations.

What is Validated? Performance

- Performance is how well a system performs, provided that service is proper
  - Generic Performance Measures:
    - **throughput** -- the number of jobs processed per time unit
    - **response time** -- the time to process a specific job.
    - **capacity** -- the maximum number of jobs that may be processed per time unit

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

What is Validated/Measured? Dependability (I)

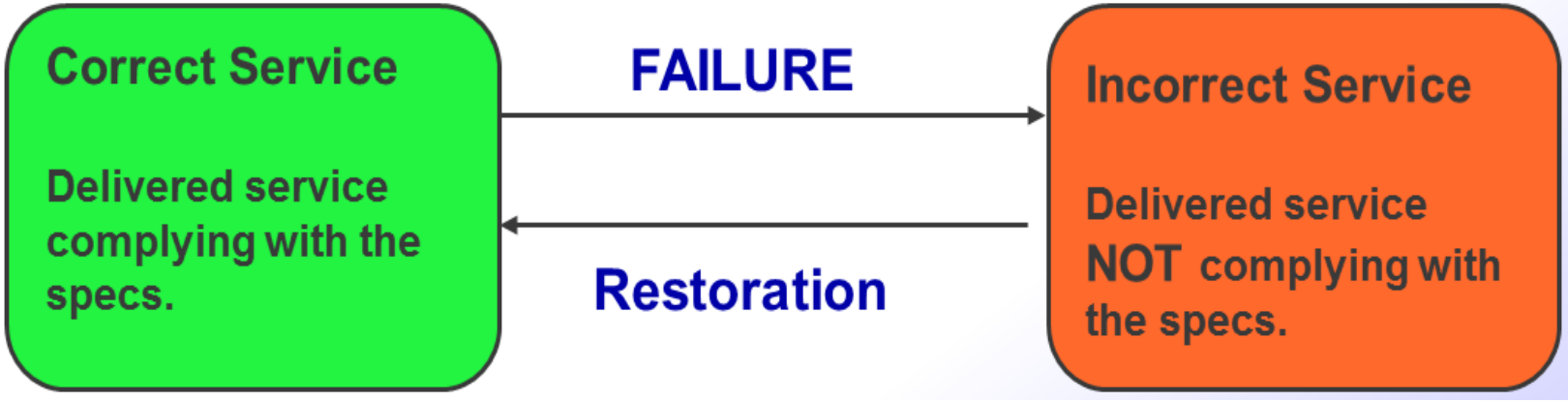
- Then, what can we Validate/Measure? Dependability
  - ability to avoid service failures that are more frequent and more severe than is acceptable

From: Avizienis, A.; Laprie, J.-C.; Randell, B.; Landwehr, C. "Basic concepts and taxonomy of dependable and secure computing" IEEE TDSC, Vol. 1 Page(s): 11- 33, 2004

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

What is Validated/Measured? Dependability (II)

- System service is proper if it is delivered as specified; otherwise, it is improper.
  - System failure is a transition from proper to improper service.
  - System restoration is a transition from improper to proper service.



UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Examples of Specifications of Proper Service

- k out of N components are functioning.
- Every working processor can communicate with every other working processor.
- Every message is delivered within T milliseconds from the time it is sent.
- All messages are delivered in the same order to all working processors.
- The system does not reach an unsafe state.
- 90% of all remote procedure calls return within x seconds with a correct result.
- 99.999% of all telephone calls are correctly routed.

Notion of **proper** service provides a specification by which to evaluate a system's dependability.

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Dependability Concepts

- **Measures** - properties expected from a dependable system
  - Availability
  - Reliability
  - Safety
  - Confidentiality
  - Integrity
  - Maintainability
  - Coverage

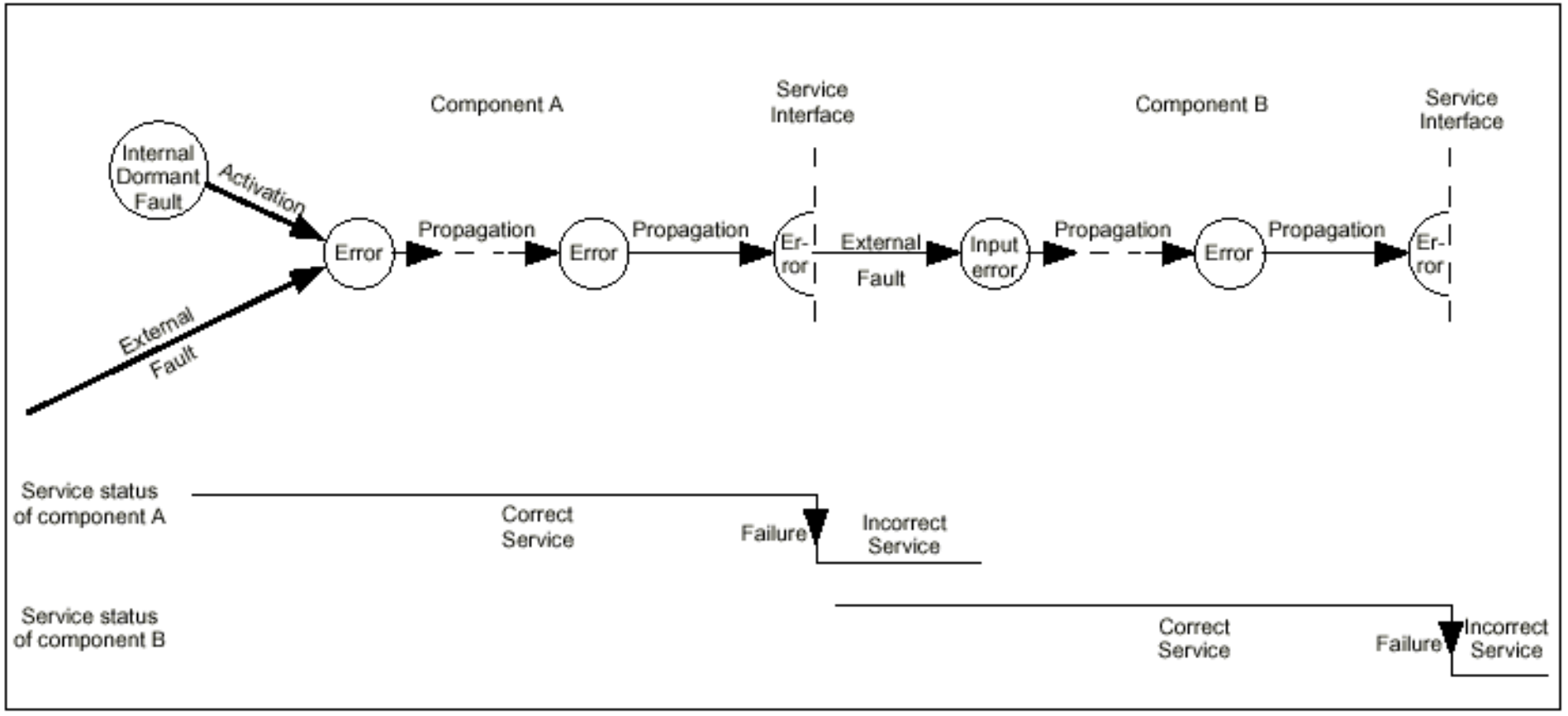
- **Means** - methods to achieve dependability
  - Fault Avoidance
  - Fault Tolerance
  - Fault Removal
  - Dependability Assessment

- **Threats** - causes of undependable operation
  - Faults
  - Errors
  - Failures

Threats: Faults, Errors and Failures

- A system may fail either because it does not comply with the specification, or because the specification did not adequately describe its function.
  - Error: that part of the system state that may cause a subsequent failure
  - A Failure occurs when an error reaches the service interface and alters the service.
  - Fault: the adjudged or hypothesized cause of an error.
- A fault is active when it produces an error; otherwise it is dormant.

Fault - Error - Failure Chain



The Means to Attain Dependability

- The development of a dependable computing system calls for the combined utilization of a set of four techniques:

– **fault prevention:**
  - how to prevent the occurrence or introduction of faults,

– **fault tolerance:**
  – how to deliver correct service in the presence of faults,

– **fault removal:**
  – how to reduce the number or severity of faults,

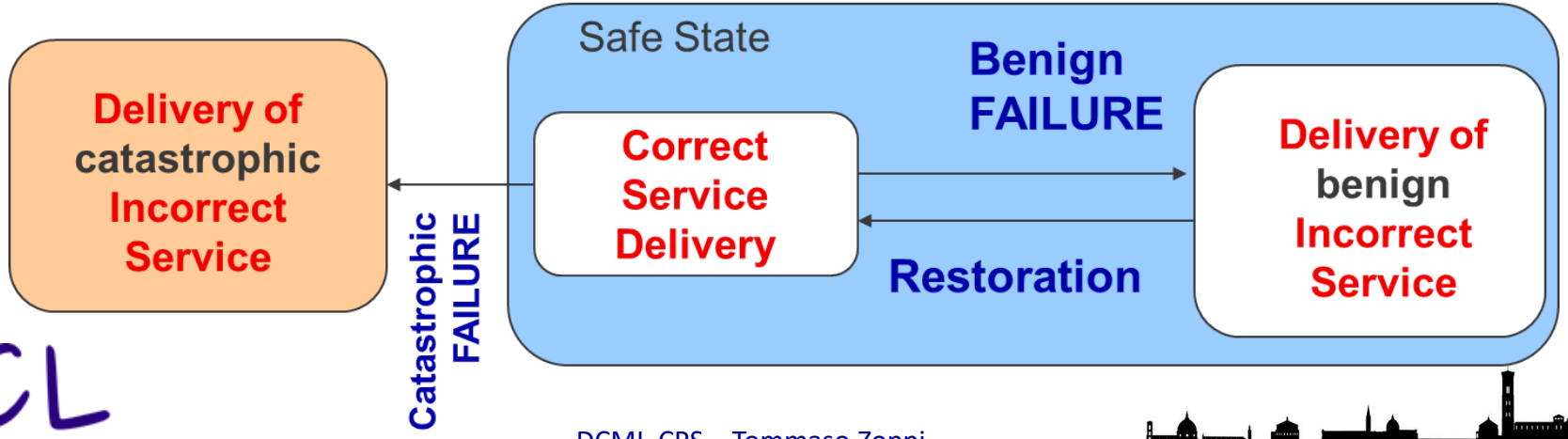
– **fault forecasting:**
  – estimate the number, the future incidence, and the likely consequences of faults.

Measures to Attain Dependability

- **Availability**: readiness for correct service.
  - quantifies the alternation between proper and improper service.
- **Reliability** - continuous delivery of service
- **Time to Failure** - measure of the time to failure from last restoration.
- **Maintainability** - ability to undergo modifications and repairs.
- **Coverage** - the probability that the system can tolerate a fault and continue to deliver proper service.

Safety

- Safety is an extension of reliability: the state of correct service and the states of incorrect service due to non-catastrophic failure are grouped into a **safe state**,
  - Safety is thus reliability with respect to catastrophic failures.
  - Safety is a measure of continuous safeness, or equivalently, of the time to catastrophic failure;



Security

- Security can be seen as a triple of
  - Availability
  - Confidentiality
  - Integrity

- Are we sure that it is just this?
  - Well, lets try to think about an attack that is not damaging neither of these attributes
  - …

On Dependability Measures

- Dependability measures are often contrasting with each other (e.g., safety and availability)
- Examples
  - A train which is always turned off into the station in a protected railway
    - Availability? Safety?
  - A nuclear power plant which works endlessly even in presence of faults
    - Availability? Safety?

Performability

- Performability: quantifies how well a system performs, taking into account behavior due to the occurrence of faults.
  - It generalizes the notion of dependability in two ways:
    - includes performance-related impairments to proper service
    - considers multiple levels of service in specification, possibly uncountable
- Performability measures are truly user-oriented, quantifying performance as perceived by users.

Original reference: J. F. Meyer, "On Evaluating the Performability of Degradable Computing Systems," Proceedings of the 8th International Symposium on Fault-Tolerant Computing, Toulouse, France, June 1978, pp. 44-49.

Safety (Critical) Systems

- A safety-critical system (SCS) or life-critical system is a system whose failure or malfunction may result in one (or more) of the following outcomes
  - death or serious injury to people
  - loss or severe damage to equipment/infrastructure
  - environmental harm
- A safety-related system comprises everything (hardware, software, and humans) involved into one or more safety functions.

Validation Techniques

Validation Techniques

- There are several choices
  - Analytical/Numerical modeling
- Combinatorial modeling
- State-based modeling
  - Simulation (including fault injection on a simulated system)
  - Measurement (including performance benchmarking and fault injection on a prototype system)
    - each with differing advantages and disadvantages

When does Validation take place?

- In all the stages of the system development process:
  - Specification
    - Analytical/Numerical modeling
  - Design
    - Analytical/Numerical modeling, Simulation modeling
  - Implementation
    - Detailed Simulation modeling, Measurement, including Fault Injection
  - Operation
    - Analytical/Numerical modeling, Detailed Simulation modeling, Measurement, including Fault Injection

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

The "Art" of Performance and Dependability Validation

- Performance and Dependability validation is an art because:
  - There is no recipe for producing a good analysis,
  - The key is knowing how to abstract away unimportant details, while retaining important components and relationships,
  - This intuition only comes from experience,
  - Experience comes from making mistakes.

There are many ways to make mistakes.

Doing it Right (I)

- Understand the desired measure
  - before you build the model or
  - design a measurement or fault-injection experiment.
  - The desired measure determines the type of model, performance benchmark, or fault-injection experiment and the level of detail required.
- No model or measurement technique is universal.

Doing it Right (II)

- Choose the desired measures:
  - Choice of measures form a basis for comparison.
  - It's easy to choose wrong measure and see patterns where none exist.
  - Measures should be refined during the design and validation process.
  - Understand the meaning of the obtained measures:
    - Numbers are not insights.

Metrology

Introduction

- The **measurement theory**, also called **metrology**, is the science of weights and measurement. It includes all *theoretical* and *practical* aspects of measurement.
- Metrology is defined by the International Bureau of Weights and Measures (abbreviated as the BIPM per the organization's French name, Bureau International des Poids et Mesures) as

  "the science of measurement, embracing both experimental and theoretical determinations at any level of uncertainty in any field of science and technology."

- Standards: International Vocabulary of Metrology (VIM), Guides to the expression of Uncertainty in Measurement (GUM) and supplements

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

VIM and GUM

- Measurement fundamentals and basic terminology
  - International vocabulary of metrology (VIM)
    - Third Edition, 2012
- Measurement uncertainty
  - The Guide to the Expression of Uncertainty in Measurement (GUM)
  - Supplement 1 to GUM - Propagation of distributions using a Monte Carlo method
  - Supplement 2 to GUM - Evaluation of measurement data – Extension to any number of output quantities
  - Documents available here:
    http://www.bipm.org/en/publications/guides/

Metric Systems

Why the metric system matters - Matt Anticole.mp4

https://www.youtube.com/watch?v=7bUVjJWA6Vw

Measurement

► Measurement

Process of experimentally obtaining one or more quantity values that can reasonably be attributed to a quantity

(called the **measurand**)

- Objective:
  - To determine the value of the measurand, that is, the value of the particular quantity to be measured.

Measurement (2)

- A measurement involves:
  - a description of the quantity (the **measurand**) commensurate with the intended use of a measurement result
  - a measurement procedure
  - a calibrated measuring system that operates in accordance with the measurement procedure in the specified measurement conditions

Measurand

- **Measurand**

  Quantity intended to be measured

  - The specification of a measurand requires knowledge of the **kind of quantity**, description of the state of the phenomenon, body, or substance carrying the quantity, including any relevant component, and the chemical entities involved

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Lets Think About Examples

- Think about your body temperature
  - Define a Measurement System
    - And a Measurement Procedure
- Which are the properties of this procedure?
  - Should I always use the same measurement system? Why?
  - What if I use a different procedure?
  - What if I repeat the experiment tomorrow morning? Or inside/outside a building?
  - Does measuring the object affect the measurand itself?

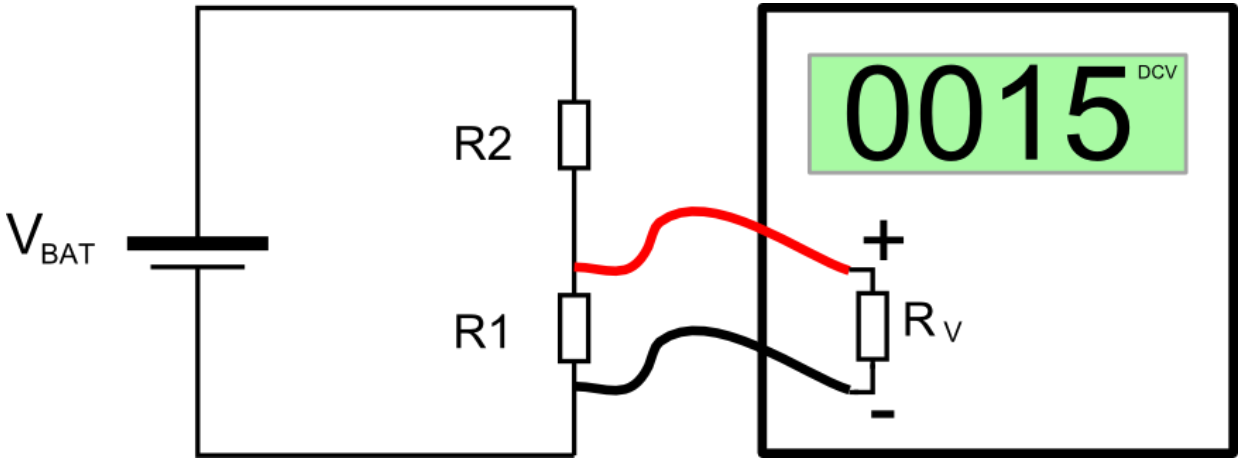
UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

On the effect of Measurement

- The measurement could induce a change in the phenomenon, body, or substance to be quantified
- This could make the quantity being measured (measurement result) different from the measurand.
- In this case, a proper correction is needed

Example - 1

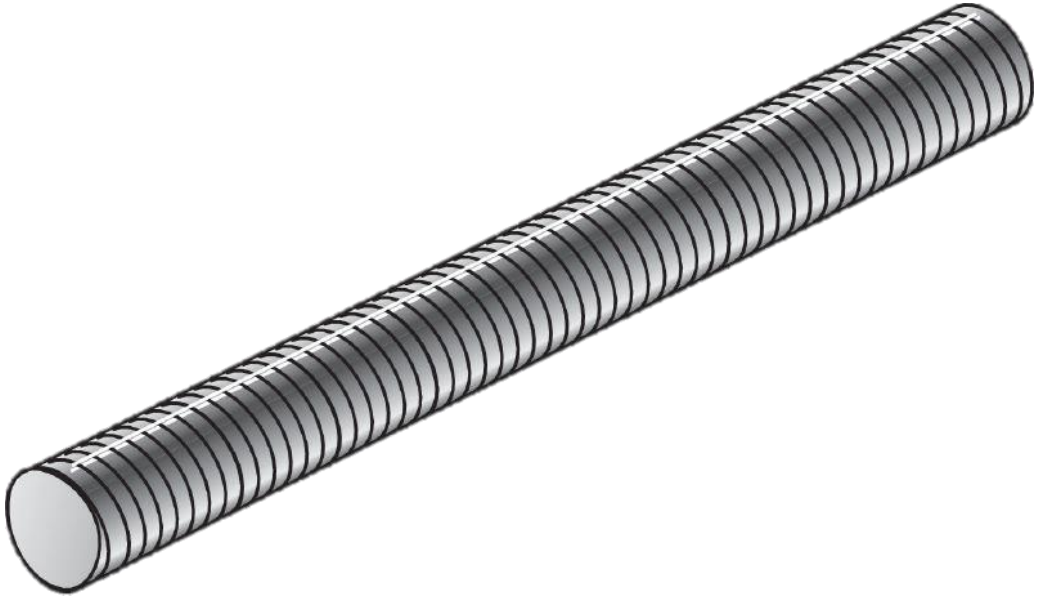
- **Example 1.** The potential difference between the terminals of a battery may decrease when using a voltmeter with a significant internal conductance to perform the measurement.



The open-circuit potential difference can be calculated from the internal resistances of the battery and the voltmeter.

Example - 2

- **Example 2.** The length of a steel rod in equilibrium with the ambient Celsius temperature of 23 °C will be different from the length at the specified temperature of 20 °C, which is the measurand.



Measurement Result

- Measurement result:
  - set of quantity values being attributed to a measurand
- A measurement result includes any other information that is useful and relevant about the set of quantity values
  - E.g. some values are more representative of the measurand than others (represented in the form of a probability density function)

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

Measurement Result (2)

- A measurement result is generally expressed as a

  single measured quantity value

  and a

  measurement uncertainty

- The measurement result can also be expressed as a single measured quantity value. This happens when the measurement uncertainty can be considered to be negligible.
  - In many fields this is the usual way of expressing a measurement result

Measurement Characteristics - 1

- **Measurement precision**
  - closeness of agreement between indications or measured quantity values obtained by **replicate measurements on the same or similar objects under specified conditions**
- **Measurement accuracy**
  - closeness of agreement between a measured quantity value and a **true quantity value** of a measurand
- **Resolution**
  - smallest variation in a quantity being measured that is **responsible for change in the indication** (output) of the instrument

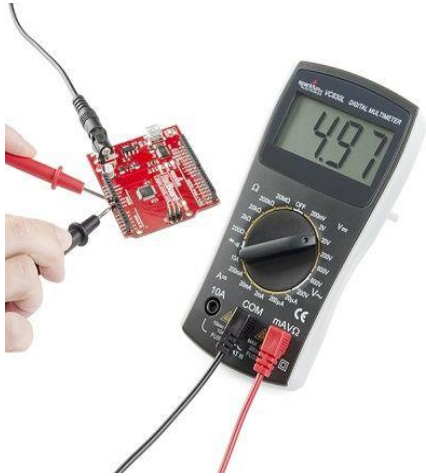
Measurement Characteristics - 2

- Repeatability condition of measurement
  - Condition of measurement that includes:
    - the same measurement procedure,
    - the same measuring system,
    - the same operating conditions,
    - the same operators,
    - the same location,

    and replicate measurements on the same or similar objects over a short period of time
- Measurement repeatability
  - measurement precision under a set of repeatability conditions of measurement

Measurement Characteristics - 3

- **Intrusiveness**
  - Not explictly defined in the standards
  - A measurement system usually affects the measurement results, which becomes different from the measurand
  - We need to minimize and assess it



- **Measurement Time**
  - It is strictly related with the costs
  - It provides an **upper bound** of the number of measurements that can be perfomed per unit of time

UNIVERSITÀ DEGLI STUDI FIRENZE
DIMAI
DIPARTIMENTO DI MATEMATICA E INFORMATICA "ULISSE DINI"

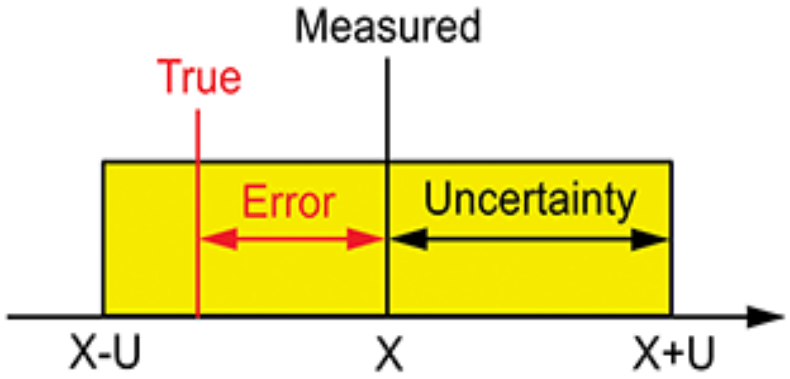
Example: Measuring System Indicators

- Suppose you want to measure some performance indicators of the system (e.g., CPU / RAM / Disk). Try to define
  - the measurand
  - a measurement procedure
  - a calibrated measuring system and its resolution
  - Do you expect accurate measures?
  - Do you expect precise measures?

- Is the measurement system intrusive? Why?
  - If yes, define a process to estimate intrusiveness

Measurement Error

- A measurement generally has flaws that can lead to an error in the measurement result
- The **measurement error** is defined as measured quantity value minus a reference quantity value



- Which reference quantity value? The true value.
- Thus, the error is unknowable!

Measurement Error (2)

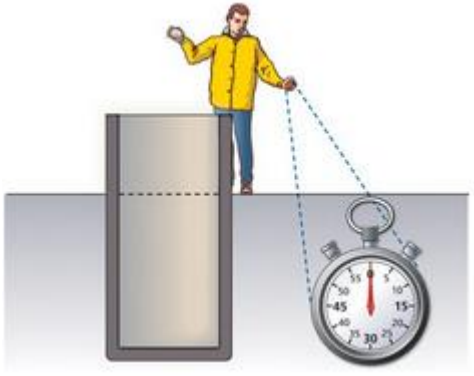
- However, a part of it can be estimated
  - and, therefore, corrected
- A measurement error consists of two parts: a systematic one and a random one

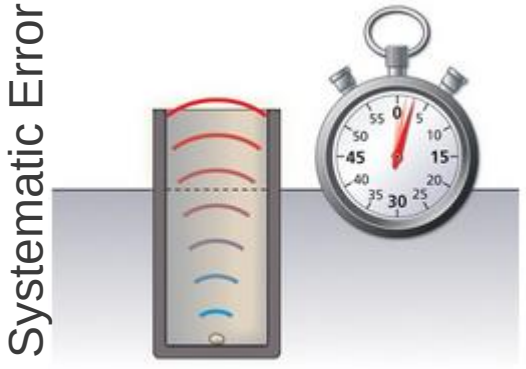
  Measurement error = Systematic error + Random error

Systematic Error

- **Systematic error:** component of the measurement error that either does not vary or varies in a predictable way
  - Typically caused by imperfect calibration of measurement instruments or imperfect methods of observation, or interference of the environment with the measurement process

Example: how long does it take a stone to reach the bottom of a well where we can not see the end ...



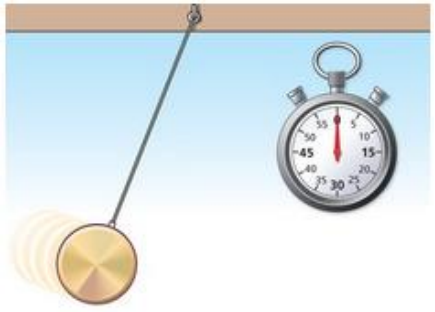


Can it be reasonably estimated?

Random Error

- **Random error:** component of measurement error that varies in a unpredictable manner when replicating measurements
  - It is reasonable to think that random error is due to unpredictable or random variations of influence quantities, which in their turn cause variations in repeated observations of the measurand

Example: when measuring time needed for a pendulum to go from one place to another, we could start the timer late, or ahead of the beginning of the first oscillation.



Can it be reasonably estimated?

Measurement Error: Summary

- A measurement result, even when the systematic errors have been corrected, is still an estimation of the measurand due to
  - Random errors
  - Not perfect correction of systematic errors

- The Guide to the Expression of Uncertainty (GUM) assumes that the result of a measurement has been corrected for all recognized significant **systematic effects** and that every effort has been made to identify such effects,
  - **before the uncertainty can be evaluated**

What Uncertainty is?

- Sometimes, it is a positive aspect
  - See http://jhollands.co.uk/journal/uncertainty-in-games-by-greg-costikyan-of-playdom/
  - "If you're not uncertain of what's going to happen in a game, why even bother playing? Look at Tic Tac Toe – we're all tired of it because we know exactly how to win. If both players know the old trick, then it's a draw. Most adults are certain that a game of nought's and crosses will result in a tie, and so it is not fun".
- Which uncertainties are in games?

What Uncertainty is? (cont.)

- Sometimes, it is a positive aspect
  - See http://jhollands.co.uk/journal/uncertainty-in-games-by-greg-costikyan-of-playdom/
- Which uncertainties are in games?

–**Performative Uncertainty**

–**Solver Uncertainty**

–**Schedule Uncertainty**

–**Narrative Uncertainty**

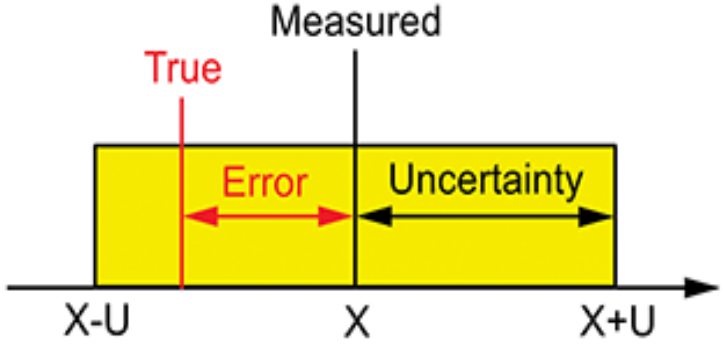
–**Feature Uncertainty**

–**Player Uncertainty**

Measurement Uncertainty

When measuring, uncertainty is UNDESIRED!

- **It is defined as a non-negative parameter characterizing the dispersion of the quantity values being attributed to a measurand, based on the information used**
  - The parameter may be, for example, a **standard deviation** called standard measurement uncertainty (or a specified multiple of it), or the half-width of an interval, having a stated coverage probability



Sources of Uncertainty

- When measuring, multiple uncertainties may pop up:
  - Incomplete definition of the measurand
  - Unrepresentativeness of the samples with regard to the measurand
  - Inadequate knowledge of the effects of the environment on the measurement, or imperfect measurement of such effects
  - Bias of the operator in reading (analog instrumentation)
  - … and many others

Measurement Uncertainty (2)

- The result of a measurement is **the best estimate** we can do for the measurand.
- We complete it with information on the set of values that can be reasonably attributed to the measurand
- The uncertainty depends on our degree of knowledge, on the amount of information that we have
  - The concept is radically different from the **error**

Standard and Expanded Uncertainty

- **Standard Uncertainty**: uncertainty of the result of a measurement expressed as a **standard deviation**

$$\bar{x} - s < x < \bar{x} + s$$

- **Expanded Uncertainty**: quantity defining an interval about the result of a measurement that may be expected to encompass a large fraction of the distribution of values that could reasonably be attributed to the measurand. It is obtained by multiplying the standard uncertainty by a **coverage factor k**.

$$\bar{x} - ks < x < \bar{x} + ks$$

- → k is the **coverage factor** and it is used to define the **confidence interval**

To Sumamrize: a nice video

- For the Love of Physics (Walter Lewin's Last Lecture)
  - https://www.youtube.com/watch?v=4a0FbQdH3dY
    - About 1 hour video overall (really interesting and fun!!!)
    - Pendulum experiment: first 19 minutes
      - **a.k.a.** "… he came in like a wrecking ball …"

For the Love of Physics (Walter Lewin's Last Lecture) (online-video-cutter.com).3gp

https://www.youtube.com/watch?v=sJG-rXBbmCc