POLITECNICO MILANO 1863

Dependable (Computing) Systems

2020 – 2021

Luca Cassano
luca.cassano@polimi.it
cassano.faculty.polimi.it/ds.html

Most of the material of these slides has been provided by Prof. Cristiana Bolchini, Politecnico di Milano, Italy

Lecturer, web page & students appointments

Luca Cassano
luca.cassano@polimi.it

cassano.faculty.polimi.it/ds.html

Students meeting:
''Officially'' on Monday 15:00 – 18:00
@DEIB, 1° Floor, Building 20, Campus Leonardo

But you can always send an email to fix an appointment

Additional lecturers

Marco Gribaudo
Probability modeling and Markov chains
marco.gribaudo@polimi.it

Manuel Roveri
Data driven anomaly detection
Manuel.roveri@polimi.it

Course calendar (tentative)

Date			Topic
Feb	23	Tu	Course introduction – perspective
	24	W	Dependability definition - properties
	25	Th	Dependability Analysis: RBDs, FTs
Mar	2	Tu	Probability models and distributions
	3	W	Markov chains & Transient analysis TCMCs
	4	Th	Discussion
	16	Tu	Discussion about dependability
	17	W	Fault types, abstraction levels
	18	Th	Dependability Analysis: Fault injection

Date			Topic
Mar	23	Tu	Discussion about fault modeling and fault injection
	24	W	Design for dependability 1
	25	Th	Design for dependability 2
	30	Tu	Data driven anomaly detection
	31	W	Data driven anomaly detection - II
Apr	1	Th	Discussion
	7	W	Discussion about design for dependability
	8	Th	Course closing & projects presentation

Luca Cassano
Marco Gribaudo
Manuel Roveri

Tuesday, 9:15 – 12:15, room 25.1.5
Wednesday, 15:15 – 18:15, room T.0.3
Thursday, 10:15 – 12:15, room B.5.2

Discussion sessions

You will be divided into 4 teams

- I'd like you to auto-divide yourselves into 4 teams
- It would be nice if each team has a name

Each team will be asked to read documents/papers/technical reports and prepare a presentation for the entire class

Course material

All the slides I will provide you

+

All the papers and documents we will read for discussions

+

Additional papers/books

Course evaluation

oral examination at the end of the course – reasonably at any time w.r.t. fixed dates, provided we find an agreement

OR

a project to be carried out independently, off-line, to be discussed and agreed upon with lecturer(s)

Course rule

Please, stop me whenever you have a question and ask…

…but more important…

Course rule

Please, stop me whenever you have a question and ask…

…but more important…

…please answer ‘‘yes’’ or ‘‘no’’ (or whatever) when I hask ‘‘ok?’’, ‘‘clear?’’, ‘‘capito?’’ :D

Course rule

Please, stop me whenever you have a question and ask…

…but more important…

…please answer ‘‘yes’’ or ‘‘no’’ (or whatever) when I hask ‘‘ok?’’, ‘‘clear?’’, ‘‘capito?’’ :D

CLEAR?

What dependability is?

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

Continuity of correct service

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

Readiness for correct service

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

Ability for easy maintainance

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

Absence of catastrophic consequences

What dependability is?

The ability of a system to perform its functionality while exposing:

- Reliability
- Availability
- Maintainability
- Safety
- Security

Confidentiality and integrity of data

Why dependability?

Why dependability?

A lot of effort is devoted to make sure the implementation

- matches specifications
- fulfills requirements
- meets constraints
- optimizes selected parameters (performance, energy, …)

Why dependability?

Functional Verification

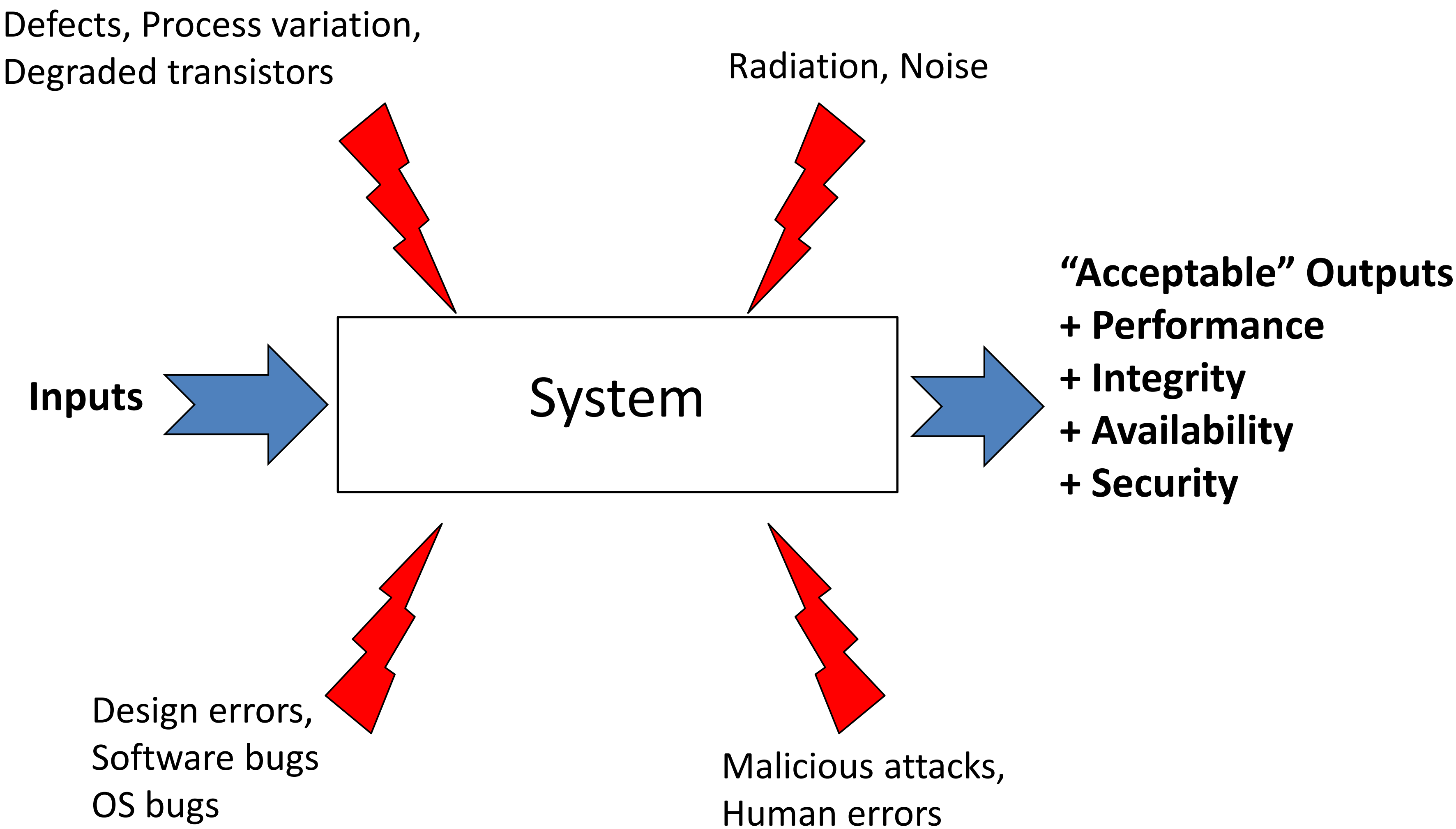
A lot of effort is devoted to make sure the implementation
- matches specifications
- fulfills requirements
- meets constraints
- optimizes selected parameters (performance, energy, …)

Nevertheless, even if all above aspects are satisfied … things may go wrong

- systems fail

systems fail … because something broke

Why dependability?



Failure effects

A single system failure may affect a large number of people

Failure effects

A failure may have high costs if it impacts economic losses or physical damage

Failure effects

Systems that are not dependable are likely not be used or adopted

Failure effects

Undependable systems may cause information loss with a high consequent recovery cost

Why dependability?

Industrial standards require it:

- ISO 26262 for automotive
- CENELEC 50128 (SW) and 50129 (HW) for railways
- RTCA DO-178C (SW) and DO-254 (HW) for airborne
- ESA ECSS-E-ST-40C (SW) and ECSS-Q-ST-60-02C (HW) for space
- ….

For the first “discussion session” you are going to read RTCA design standards…

When to think about dependability?

When to think about dependability?

Both at design-time and at runtime

Always!!!

When to think about dependability?

Both at design-time and at runtime

- Analyse the system under design
- Measure dependability properties
- Modify the design if required

When to think about dependability?

Both at design-time and at runtime

- Detect malfunctions
- Understand causes
- React

When to think about dependability?

Failures occur in development & operation

- Failures in development *should* be avoided
- Failures in operation *cannot* be avoided (things break), they must be dealt with

When to think about dependability?

Failures occur in development & operation

- Failures in development *should* be avoided
- Failures in operation *cannot* be avoided (things break), they must be dealt with

Design should take failures into account and guarantee that control and safety are achieved when failures occur

When to think about dependability?

Failures occur in development & operation

- Failures in development *should* be avoided
- Failures in operation *cannot* be avoided (things break), they must be dealt with

Design should take failures into account and guarantee that control and safety are achieved when failures occur

Effects of such failures should be predictable and deterministic … not catastrophic

Where to apply dependability?

Where to apply dependability?

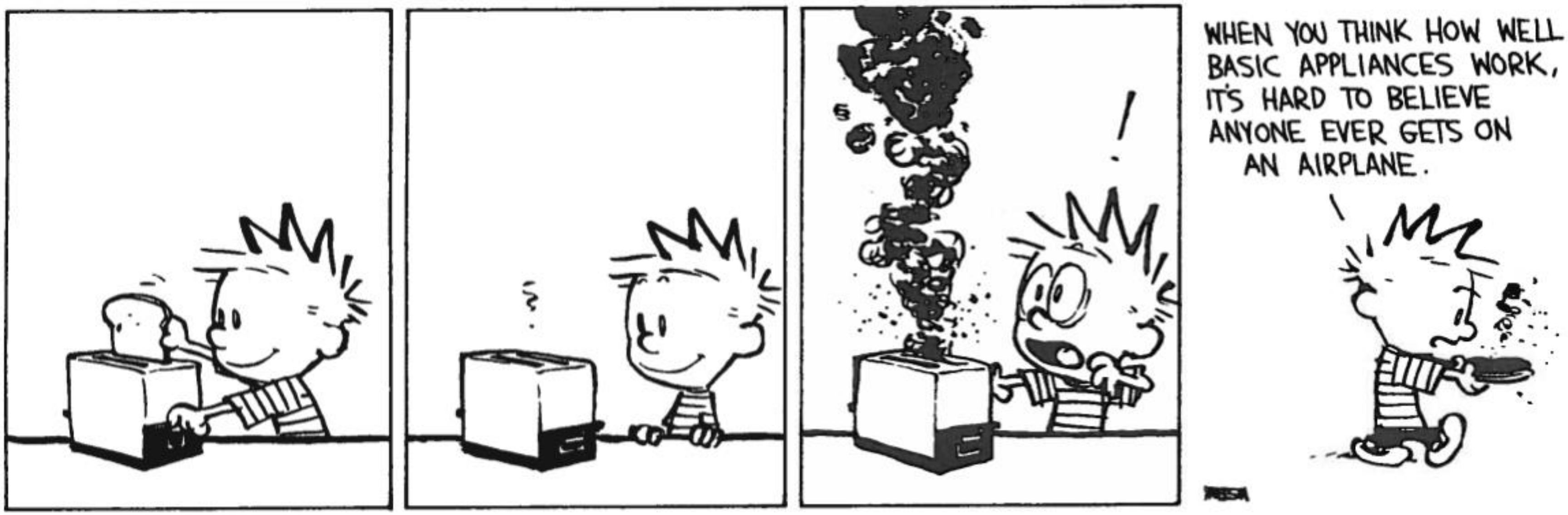
Once upon a time …

…dependability has been a relevant aspect only for safety-critical and mission-critical application environments

- Space
- Nuclear
- Avionics

Huge costs, acceptable only when mandatory …

However …



THE DAYS ARE JUST PACKED
A Calvin and Hobbes Collection by Bill Watterson

“When you think how well basic appliances work, it’s hard to believe anyone ever gets on an airplane.”

Mission-critical and safety-critical systems

Mission-critical systems: a failure during operation can have serious or irreversible effects on property and finance

- Satellites
- Surveillance drones
- Unmanned vehicles

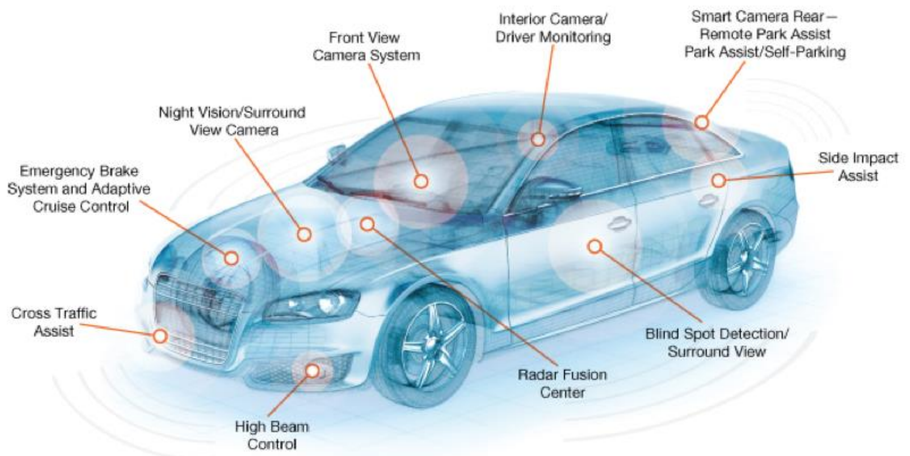
Mission-critical and safety-critical systems

Safety-critical systems: a failure during operation can present a direct threat to human life

- aircraft control systems
- medical instrumentation
- railway signaling
- nuclear reactor control systems

Today and tomorrow

Automotive

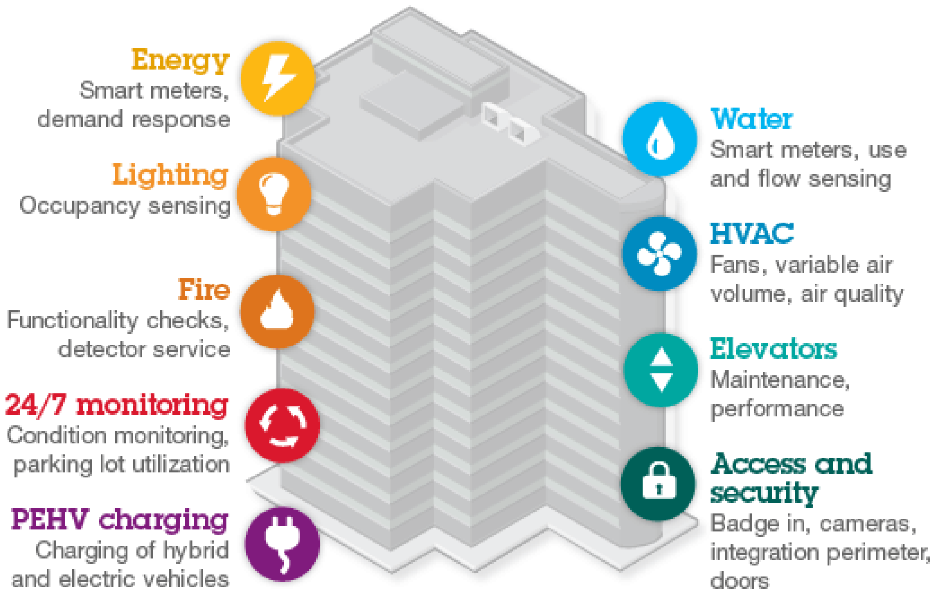


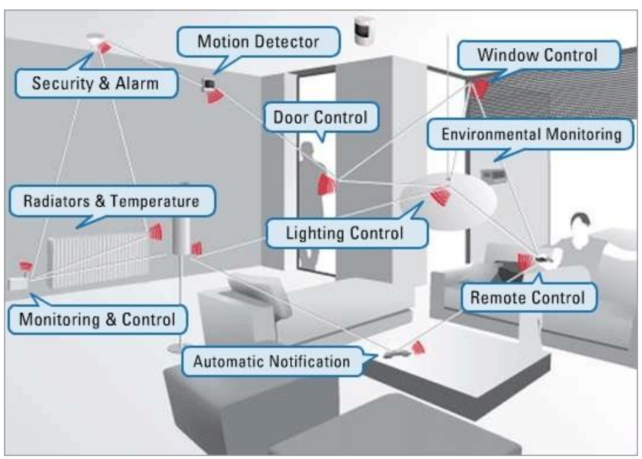
Today and tomorrow

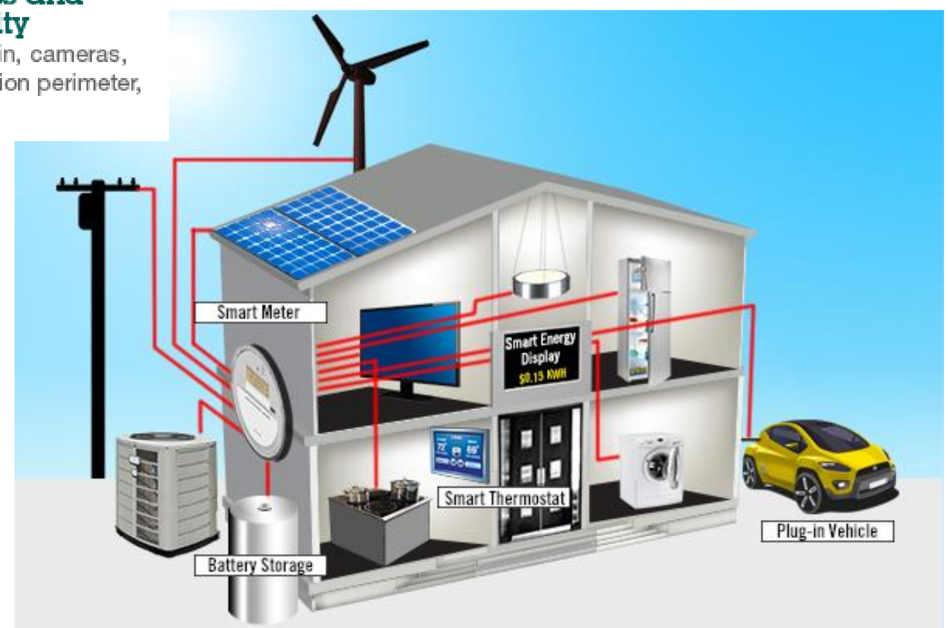
Telecommunications

Today and tomorrow

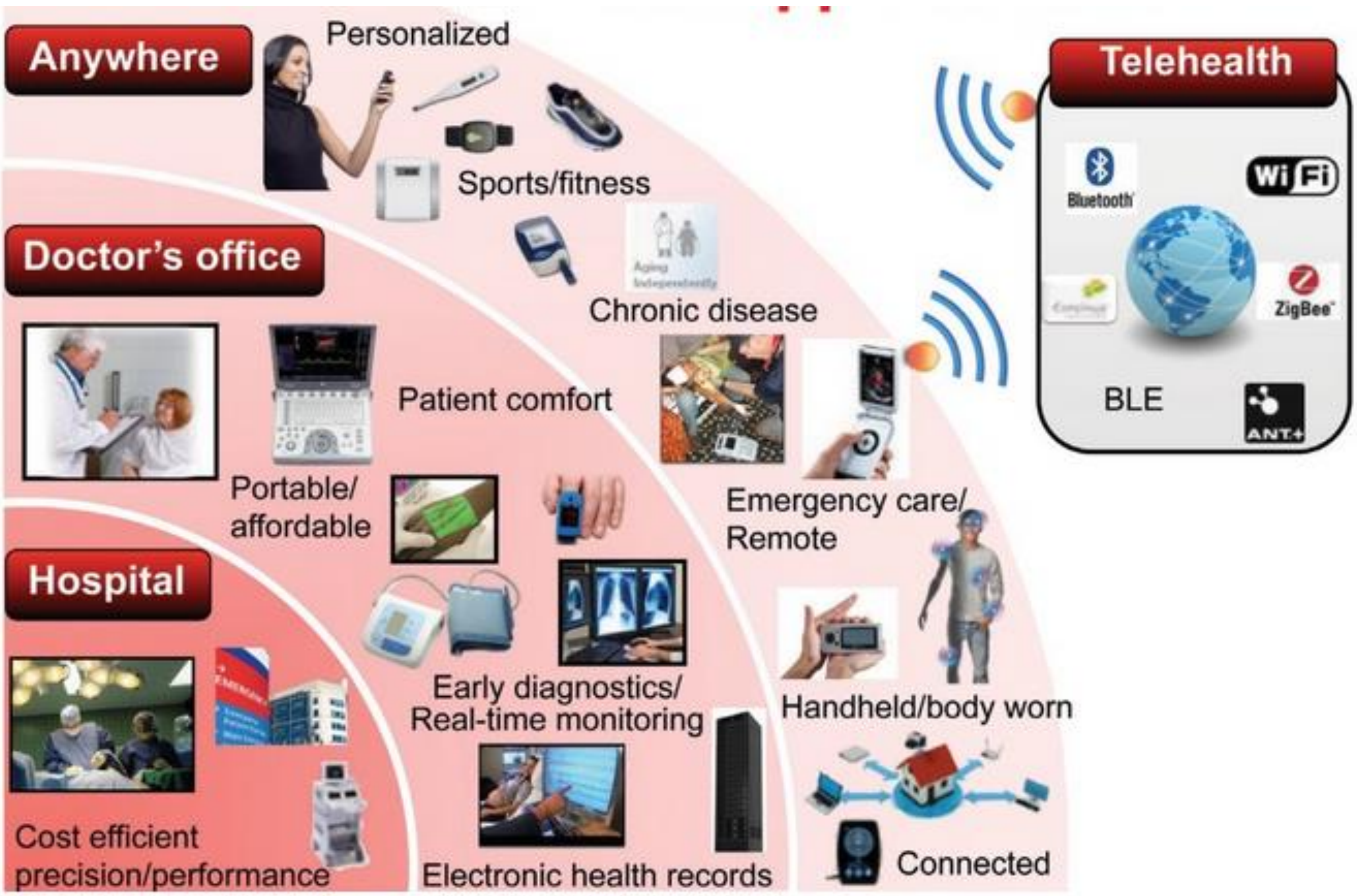
Smart spaces







Today and tomorrow



Creating solutions for health through technology innovation - Karthik Vasanth, Jonathan Sbert, Texas Instruments

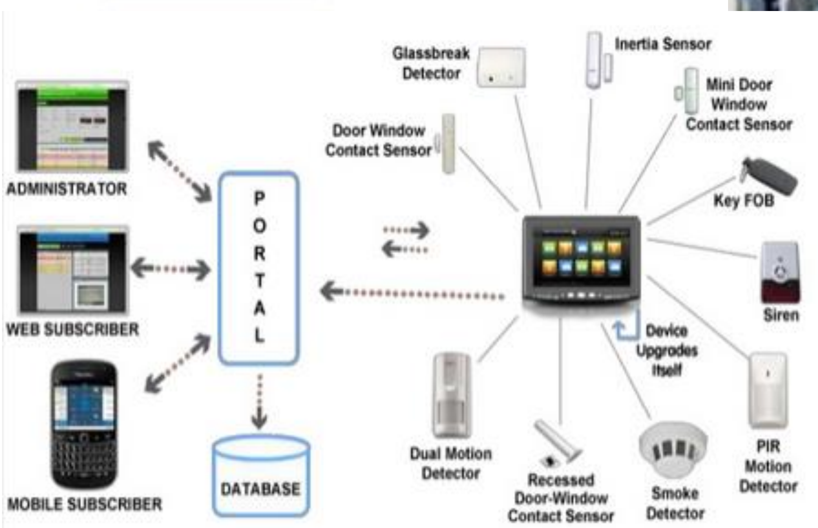
e-Health

Today and tomorrow

Logistics

Creating solutions for health through technology innovation - Karthik Vasanth, Jonathan Sbert, Texas Instruments

Today and tomorrow



Creating solutions for health through technology innovation - Karthik Vasanth, Jonathan Sbert, Texas Instruments

Anatomy of the scenarios

the nodes

- computing systems
- sensors and actuators

the communication

- network

the cloud

- data storage
- data manipulation

Everything has to work properly for the overall system to be working

How to provide dependability?

Failure avoidance paradigm

robust (computing) systems

Conservative design

Design validation

Detailed test

- Hardware
- Software

Infant mortality screen

Error avoidance

Failure tolerance paradigm

Error detection / error masking during system operation

On-line monitoring

Diagnostics

Self-recovery & self-repair

Where to work

technological level

- design and manufacture by employing reliable/robust components

    - Highest dependability

    - High cost
    - Bad performance (generally devices from old generation)

Where to work

architectural level

- integrate normal components using solutions that allow to manage the occurrence of failures

  - High dependability
  - High cost
  - Reduced performance

  } Depending on the adopted solution

Where to work

software/application level

- develop solutions in the algorithms or in the operating systems that mask and recover from the occurrence of failures

  - High dependability
  - High cost
  - Reduced performance

  Depending on the adopted solution

Where to work

What do all solutions have in common?

Where to work

What do all solutions have in common?

- Cost
- Reduced performance

You have to pay for dependability

Challenges

Find the best tradeoff between dependability and costs depending on:

- **Application field**
  - Is there a specific design standard?
  - Which degree of dependability is actually required?
  - Will failures cause human losses?
  - Which would be the monetary cost of a failure?
  - Would a failure have a “reputation cost”?
  - ….

Challenges

Find the best tradeoff between dependability and costs depending on:

- **Working scenario**
  - Are there sources of faults (radiation, ageing, heat, vibration…)?
  - Which are the nominal working conditions (and the extreme ones) for the system?
  - Are there systems connected to my system?
  - ….

Challenges

Find the best tradeoff between dependability and costs depending on:

- **Employed technologies**
  - Are the cpu, memory, interfaces free from sources of failures?
  - Are the cpu, memory, interfaces tolerant to failures?
  - Which are the components most susceptible to failures?
  - …

Challenges

Find the best tradeoff between dependability and costs depending on:

- **Algorithms and applications**
  - Are the input of the application free of inexactness?
  - Is the algorithm tolerant to a certain degree of inexactness?
  - Can the application tolerate a certain "down-time"?
  - …