FUNDAMENTALS — FAULTS AND FAILURES IN DYNAMICAL SYSTEMS —

Riccardo M.G. Ferrari
r.ferrari@tudelft.nl , DCSC (3ME)

Lecture 1.1b
22/04/2025

LECTURE SUMMARY

What are we going to talk about today ?

> A visual introduction to **Fault Diagnosis** (**FD**) and **Fault Tolerance** (**FT**)

> **Definitions** of main concepts, and **models** of dynamical systems

> A taxonomy of different kind of **faults**

A VISUAL INTRODUCTION

Why, what and how

A VISUAL INTRODUCTION

Examples of lack of fault tolerance

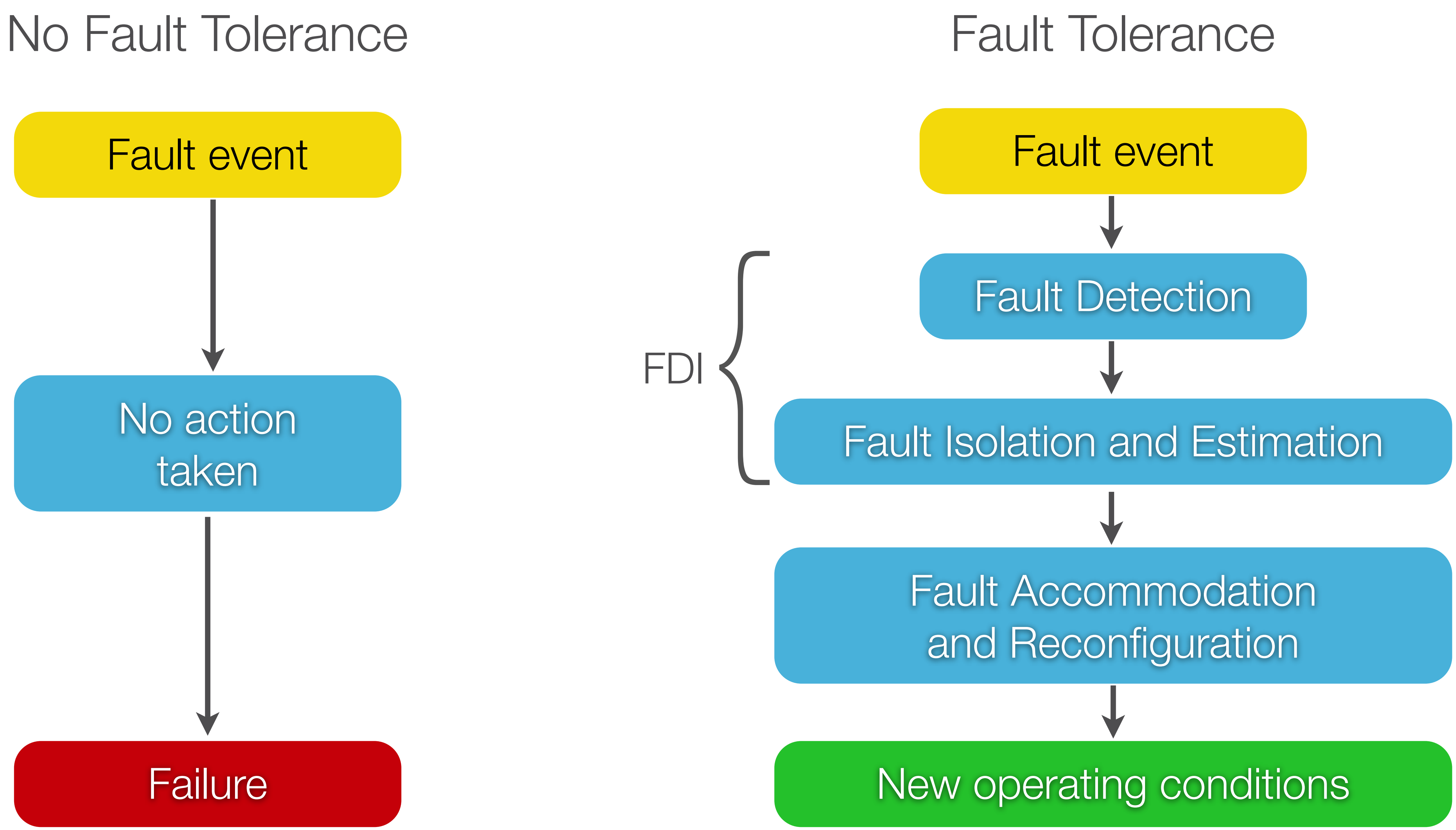
Delta II rocket

Mississippi bridge

Helicopter hydraulics failure

A VISUAL INTRODUCTION

Without, and with fault tolerance



M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault Tolerant Control*. Springer Verlag, 2006.

A VISUAL INTRODUCTION

Fault tolerance in TV fiction

You want to **land** your **ship** on **Mars**, **vertically**

This means you want to **re-orient** it, using "**reaction control thrusters**"

what if, after a 9 months trip in space, the thing **doesn't fire**?

From "**Mars**" series, copyright National Geographic (Season 1 started 2016, Season 2 premiered in 2018 and is available on Netflix)
This excerpt is freely available at https://dai.ly/x6699k0 (from time 15'07" to 23'10")

A VISUAL INTRODUCTION

Fault tolerance in TV fiction

You want to **land** your **ship** on **Mars**, **vertically**

This means you want to **re-orient** it, using “**reaction control thrusters**”

what if, after a 9 months trip in space, the thing **doesn’t fire**?

From “**Mars**” series, copyright National Geographic (Season 1 started 2016, Season 2 premiered in 2018 and is available on Netflix) This excerpt is freely available at https://www.dailymotion.com/video/x54l8cu (from time 15’07” to 23’10”)

A VISUAL INTRODUCTION

From "**Mars**" series, copyright National Geographic (Season 1 started 2016, Season 2 premiered in 2018 and is available on Netflix)
This excerpt is freely available at https://dai.ly/x6699k0 (from time 15'07" to 23'10")

A VISUAL INTRODUCTION

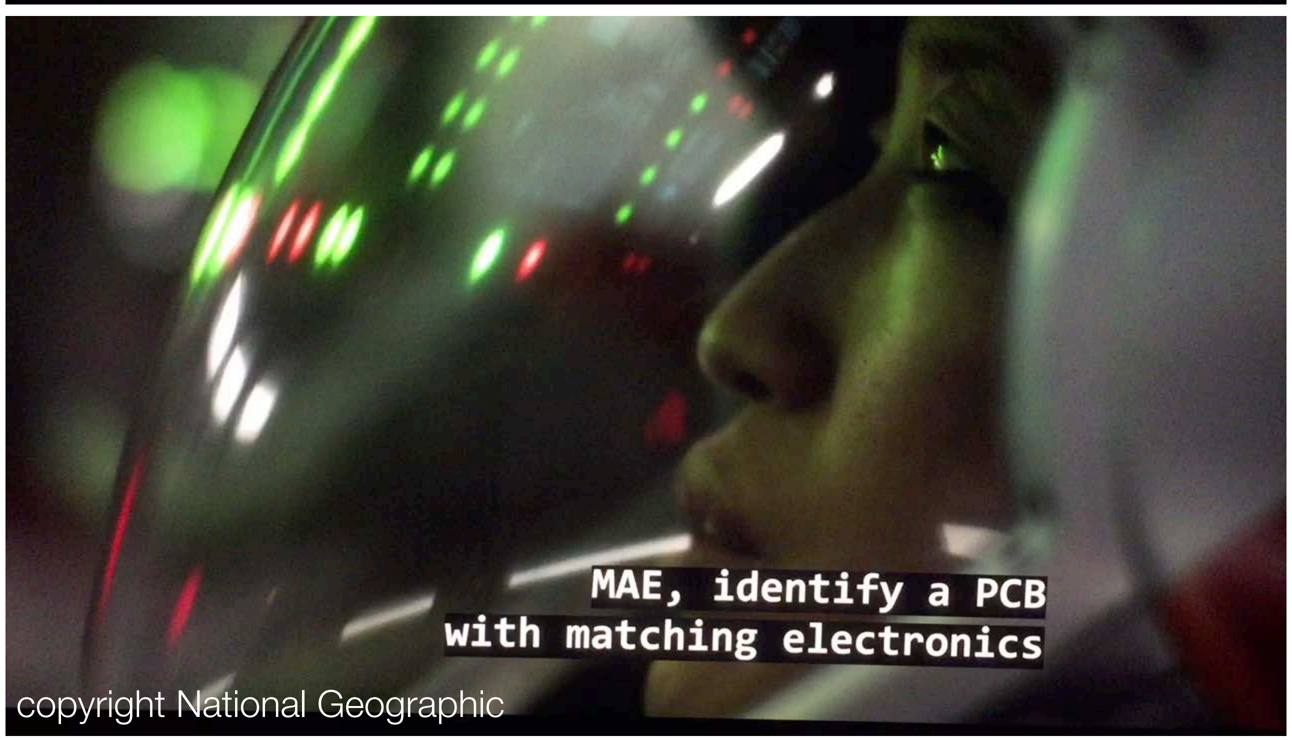
Let us review key moments, with subtitles on this time

A VISUAL INTRODUCTION

Let us review key moments, with subtitles on this time

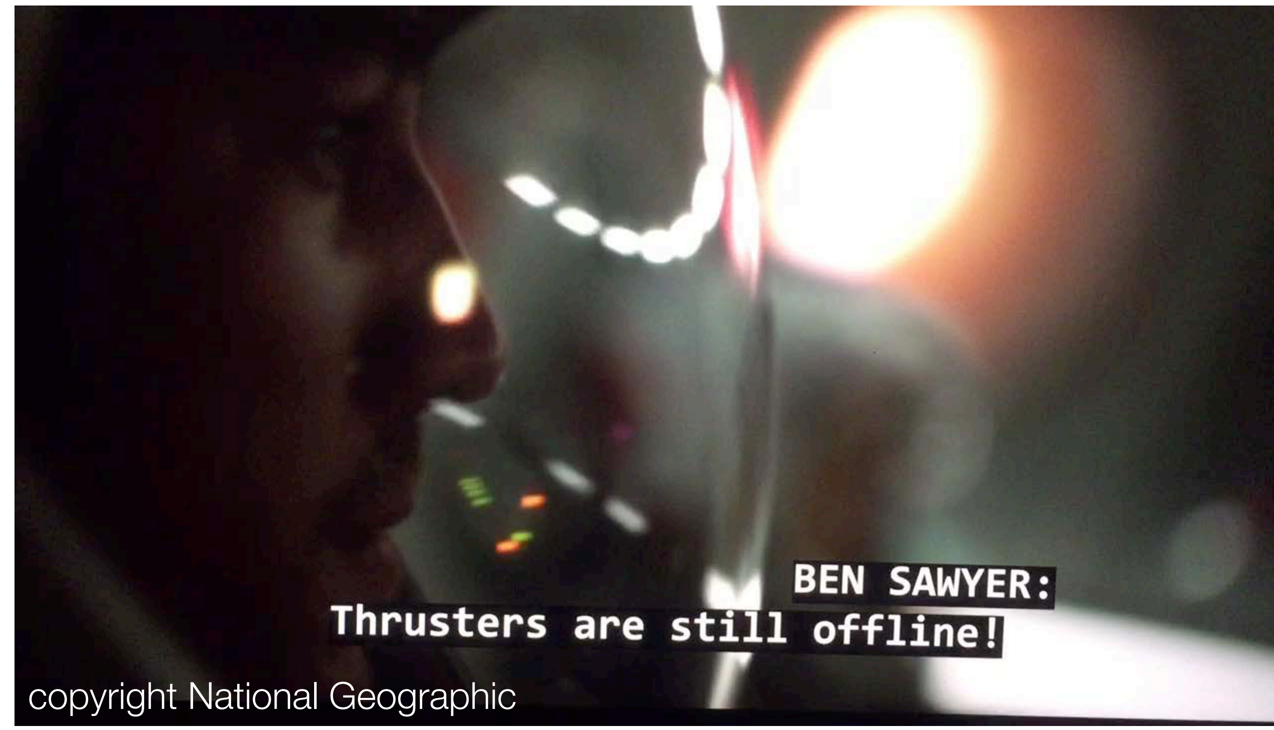
A VISUAL INTRODUCTION

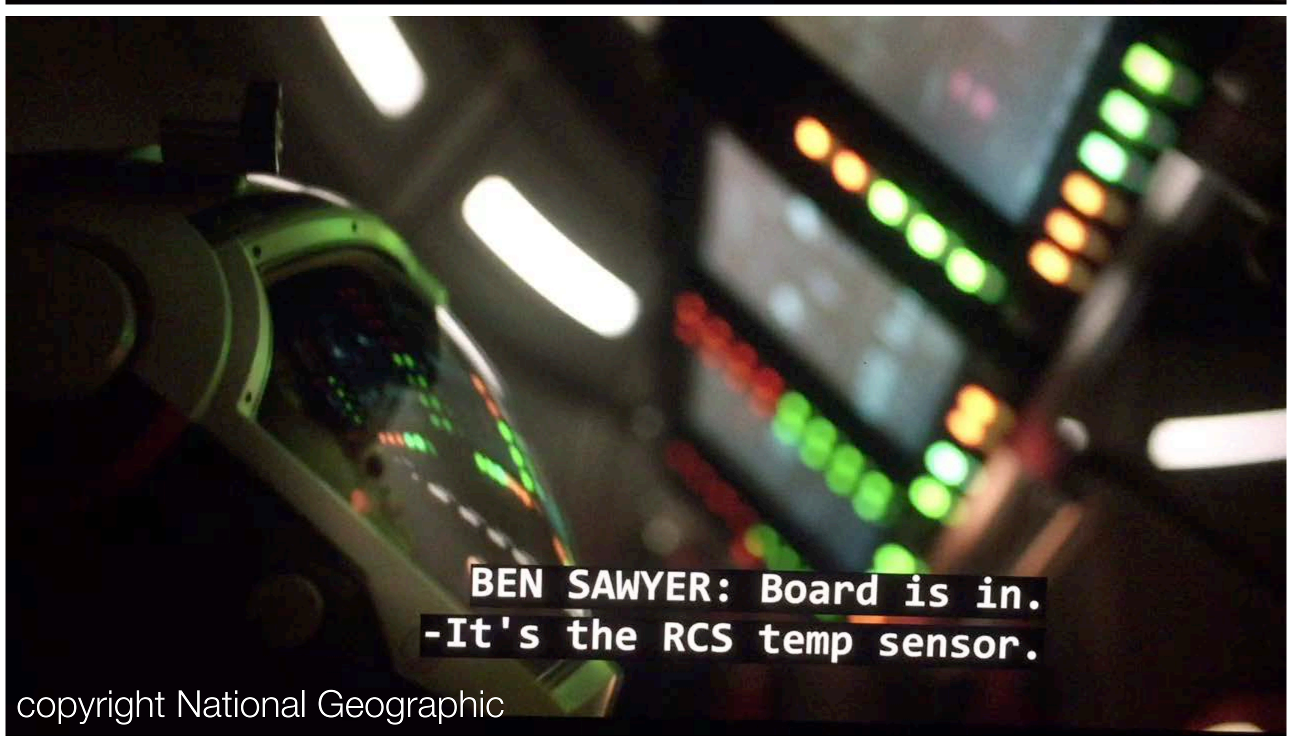
Let us review key moments, with subtitles on this time

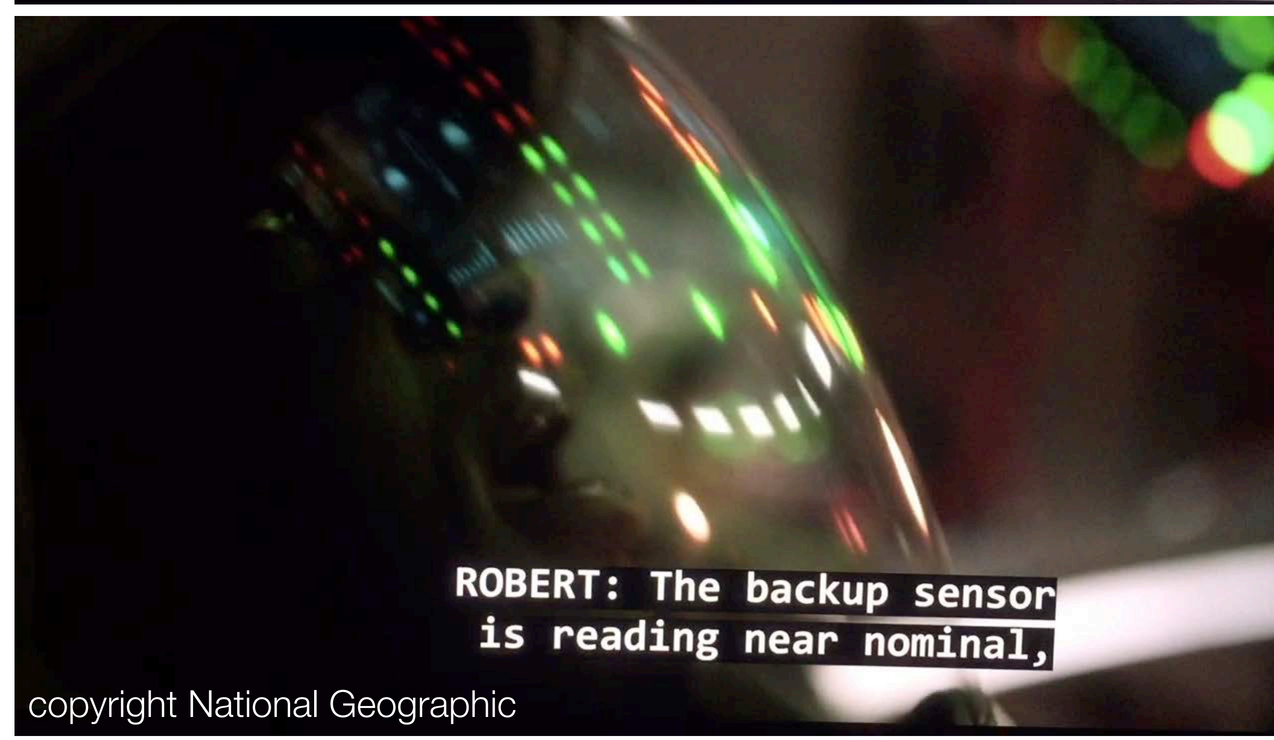


A VISUAL INTRODUCTION

Let us review key moments, with subtitles on this time

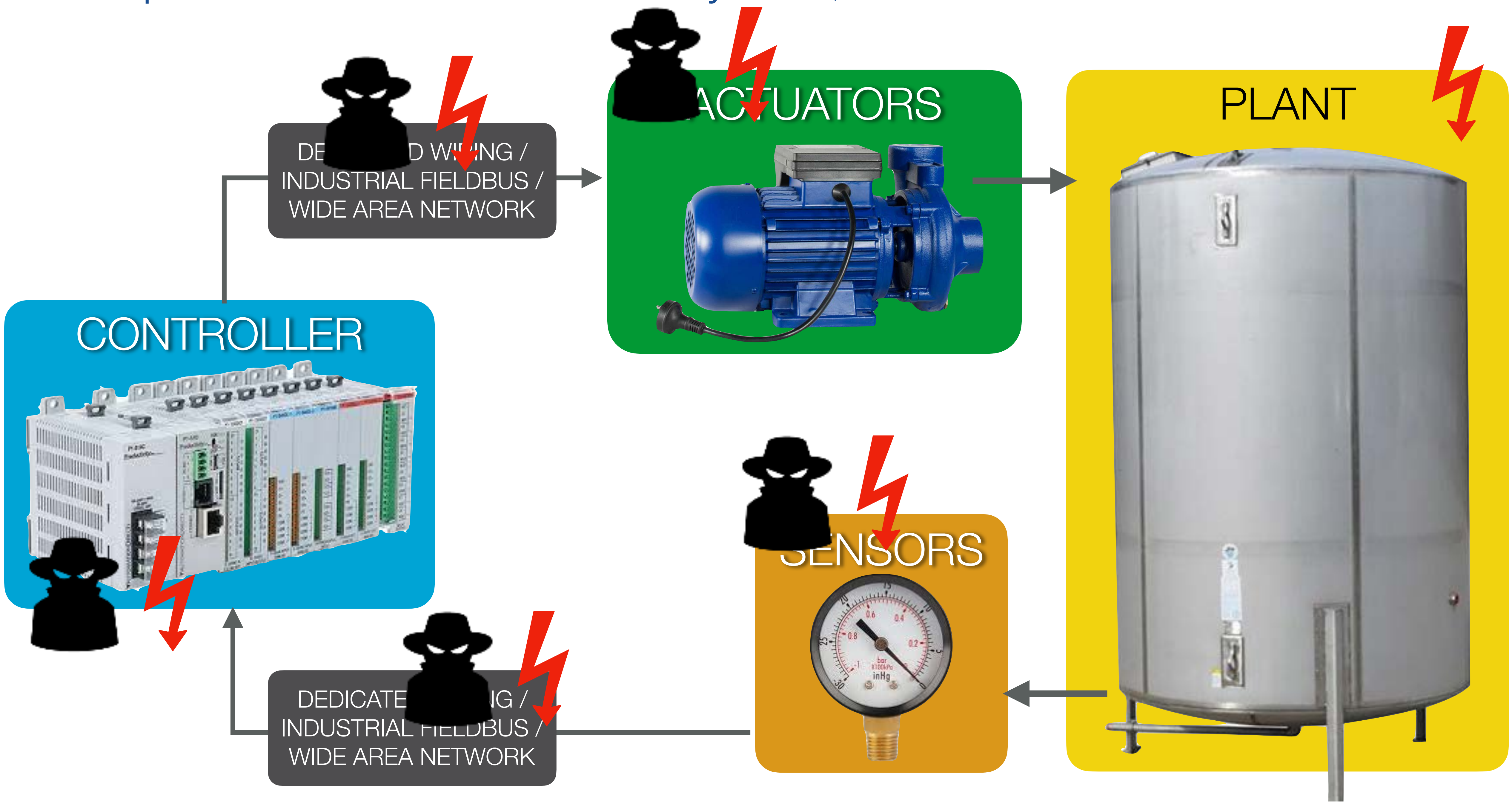






A VISUAL INTRODUCTION

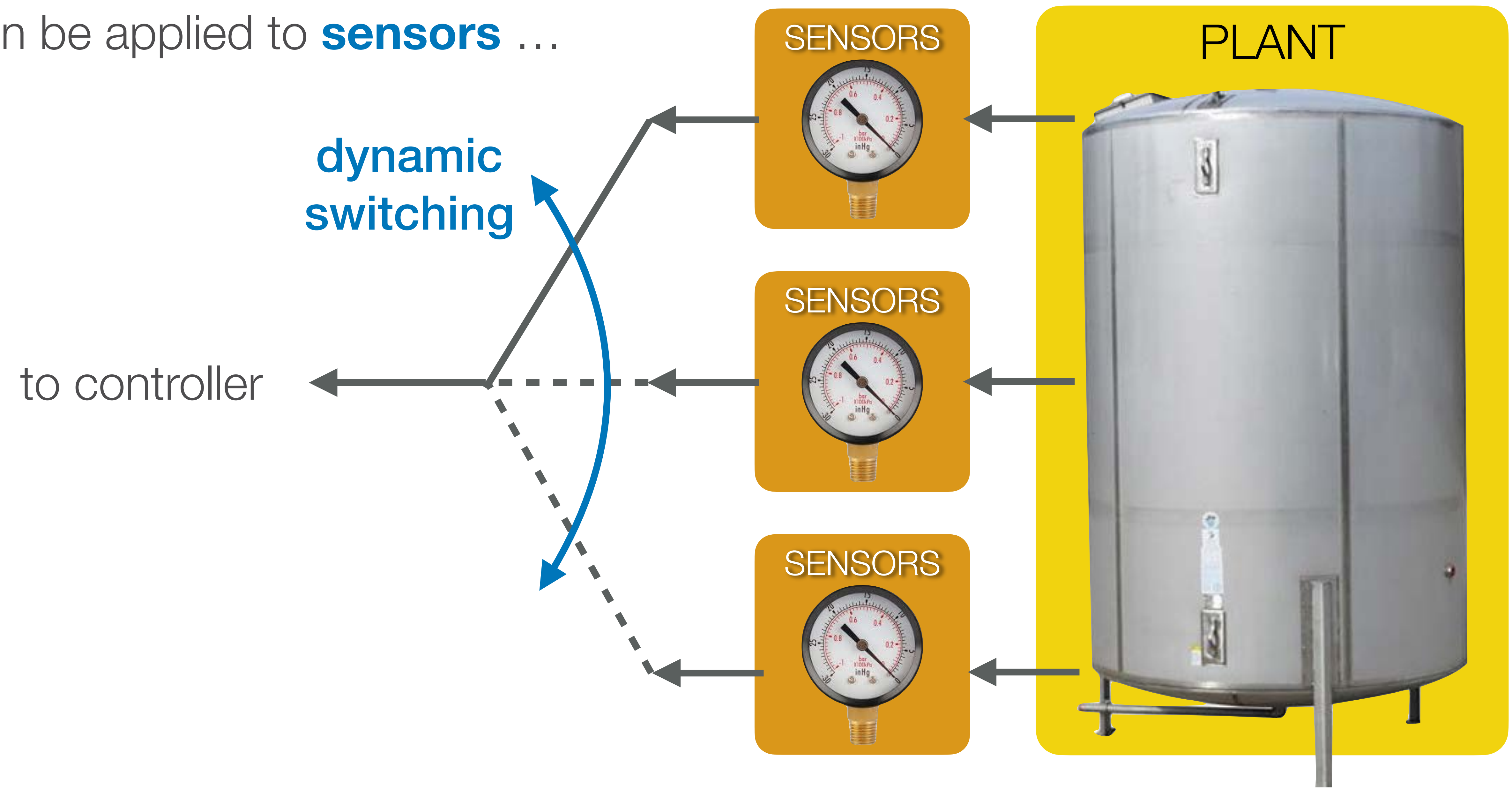
Components of an automation system, and where anomalies can strike



A VISUAL INTRODUCTION

Fault diagnosis and tolerance approach: **hardware redundancy**

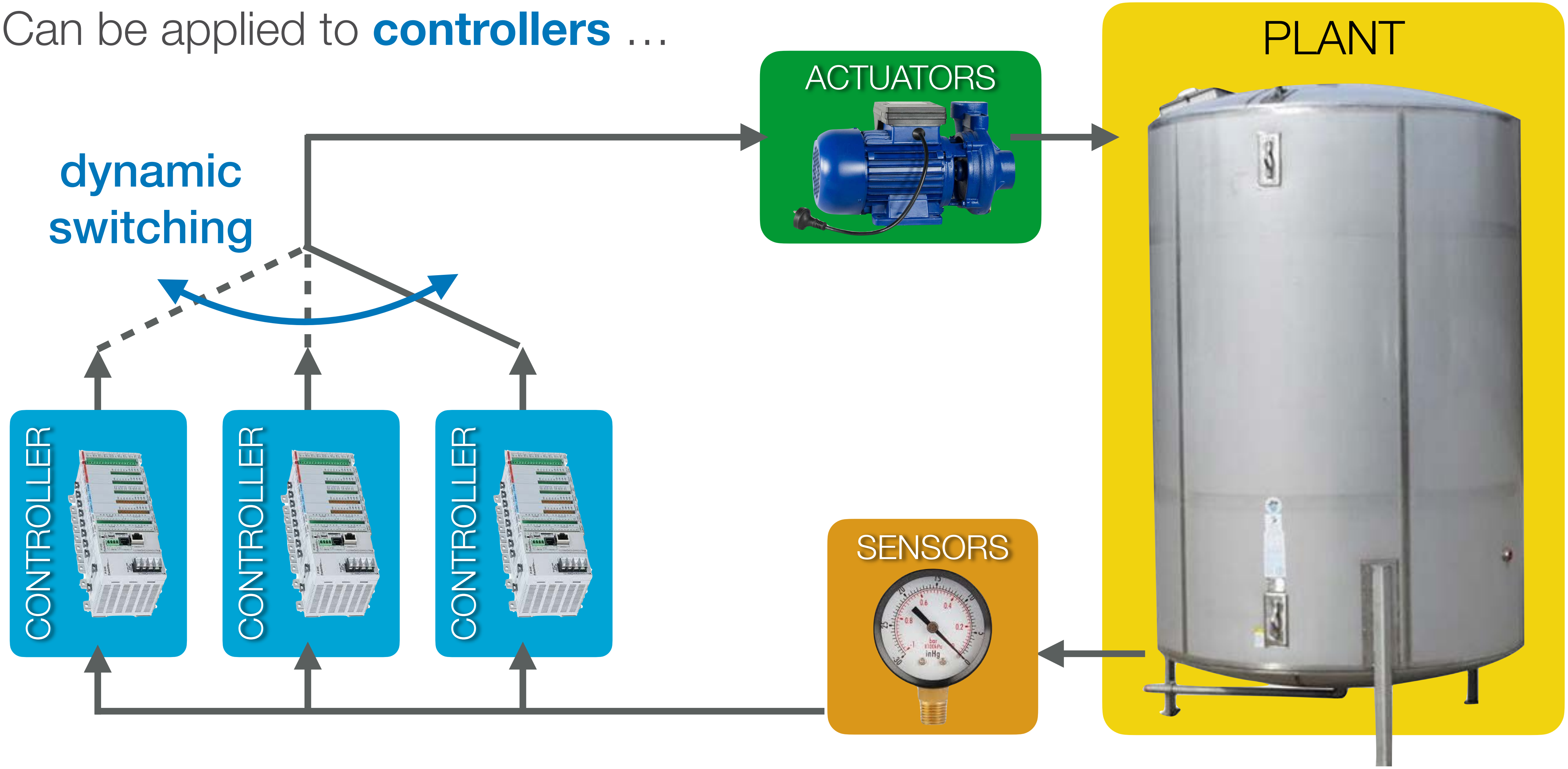
Can be applied to **sensors** …



A VISUAL INTRODUCTION

Fault diagnosis and tolerance approach: **hardware redundancy**

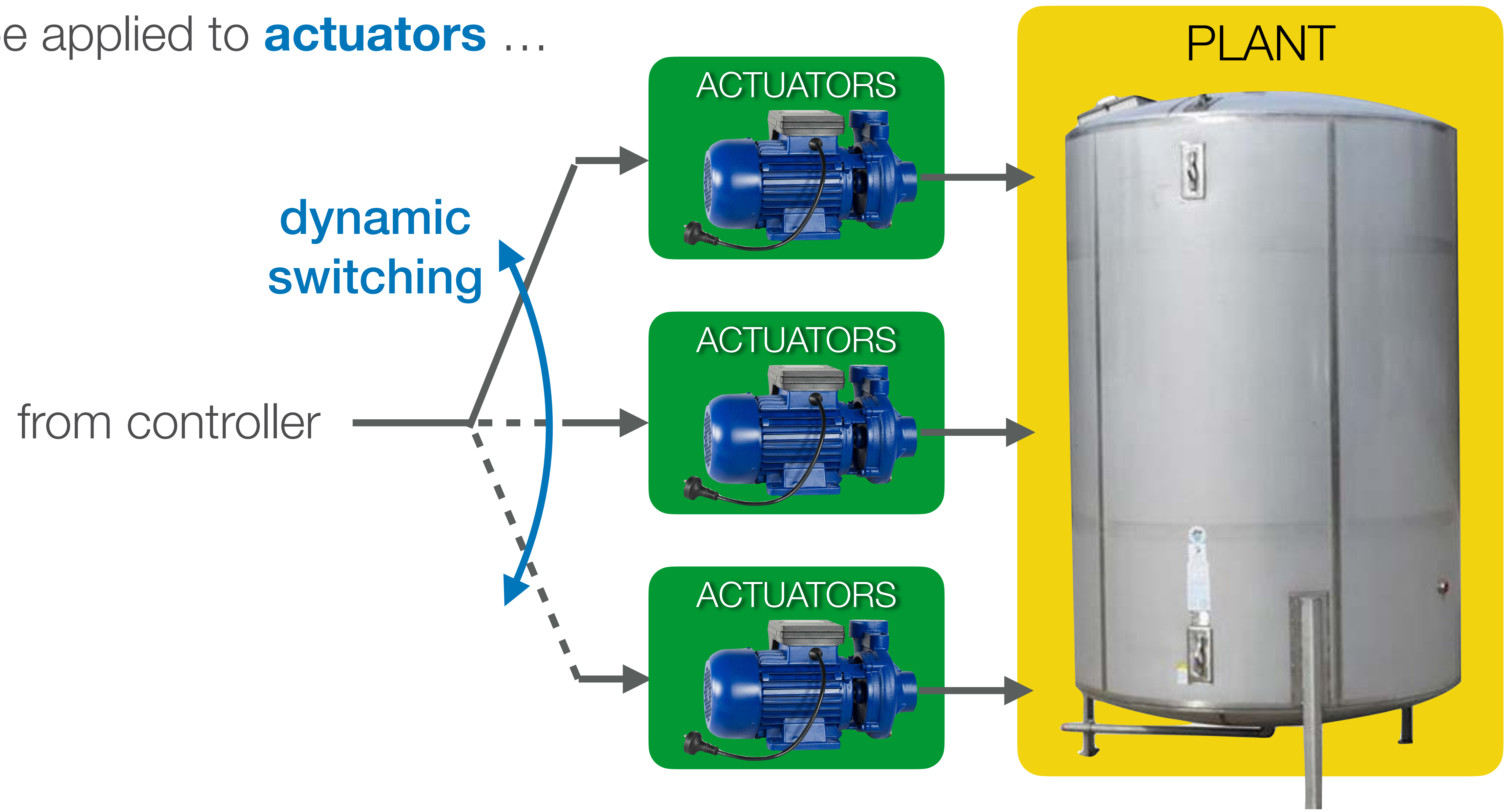
Can be applied to **controllers** …



A VISUAL INTRODUCTION

Fault diagnosis and tolerance approach: **hardware redundancy**

Can be applied to **actuators** …

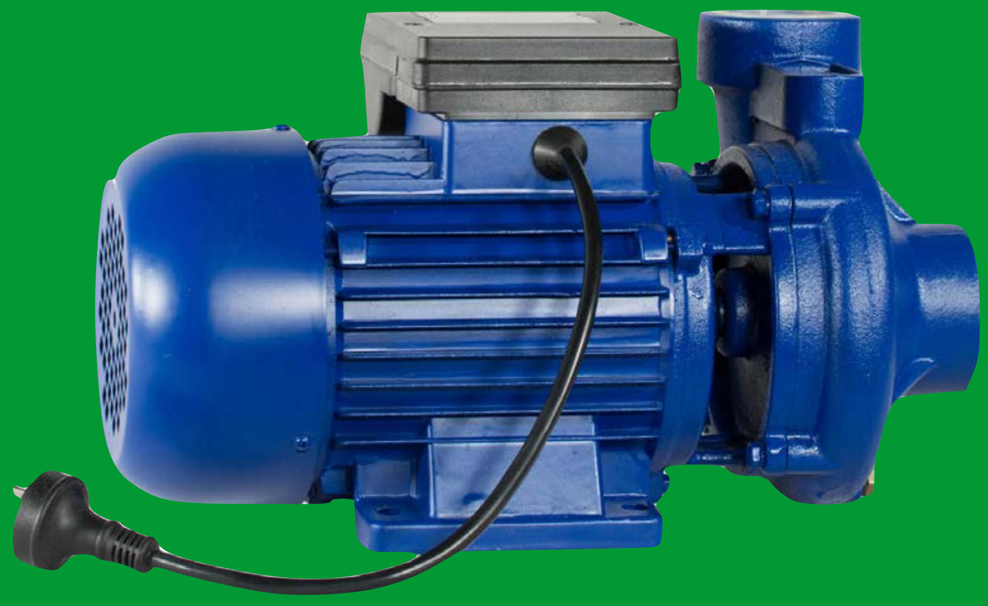


A VISUAL INTRODUCTION

A static, passive tolerance approach: **physical redundancy**

You **over-design** it, such that it cannot fail …

HUGE, STURDY ACTUATORS



PLANT

can be applied to sensors, actuators, controllers and the plant as well!

A VISUAL INTRODUCTION

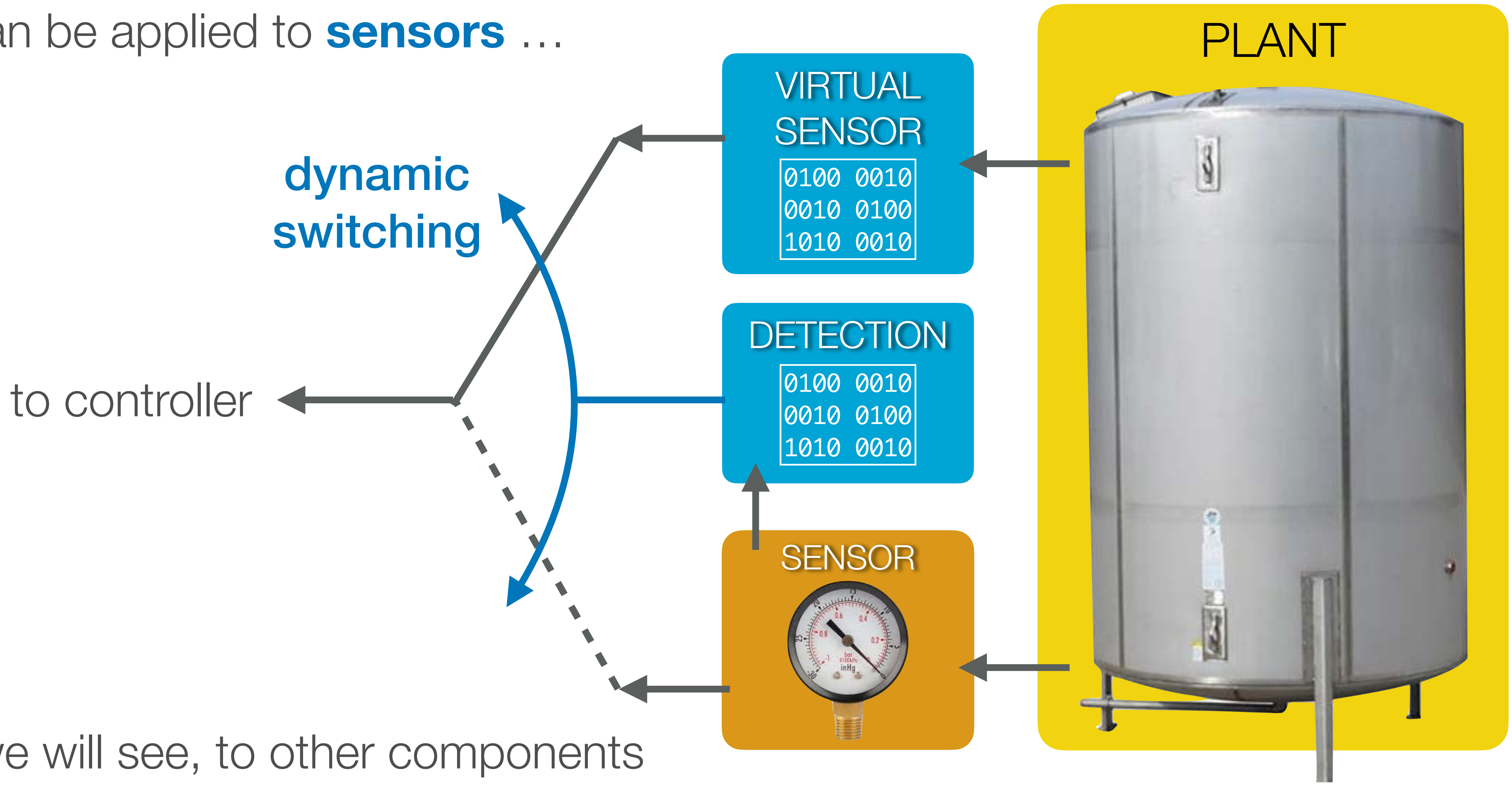
A static, passive tolerance approach: **physical redundancy**

Several natural or man-made systems have such property

A VISUAL INTRODUCTION

Fault diagnosis and tolerance approach: **analytical redundancy**

Can be applied to **sensors** …



as we will see, to other components as well (at least for diagnosis!)

OPEN QUESTION

Pros and cons of different kind of redundancies?

	Hardware	Physical	Analytical
Pro			
Cons			

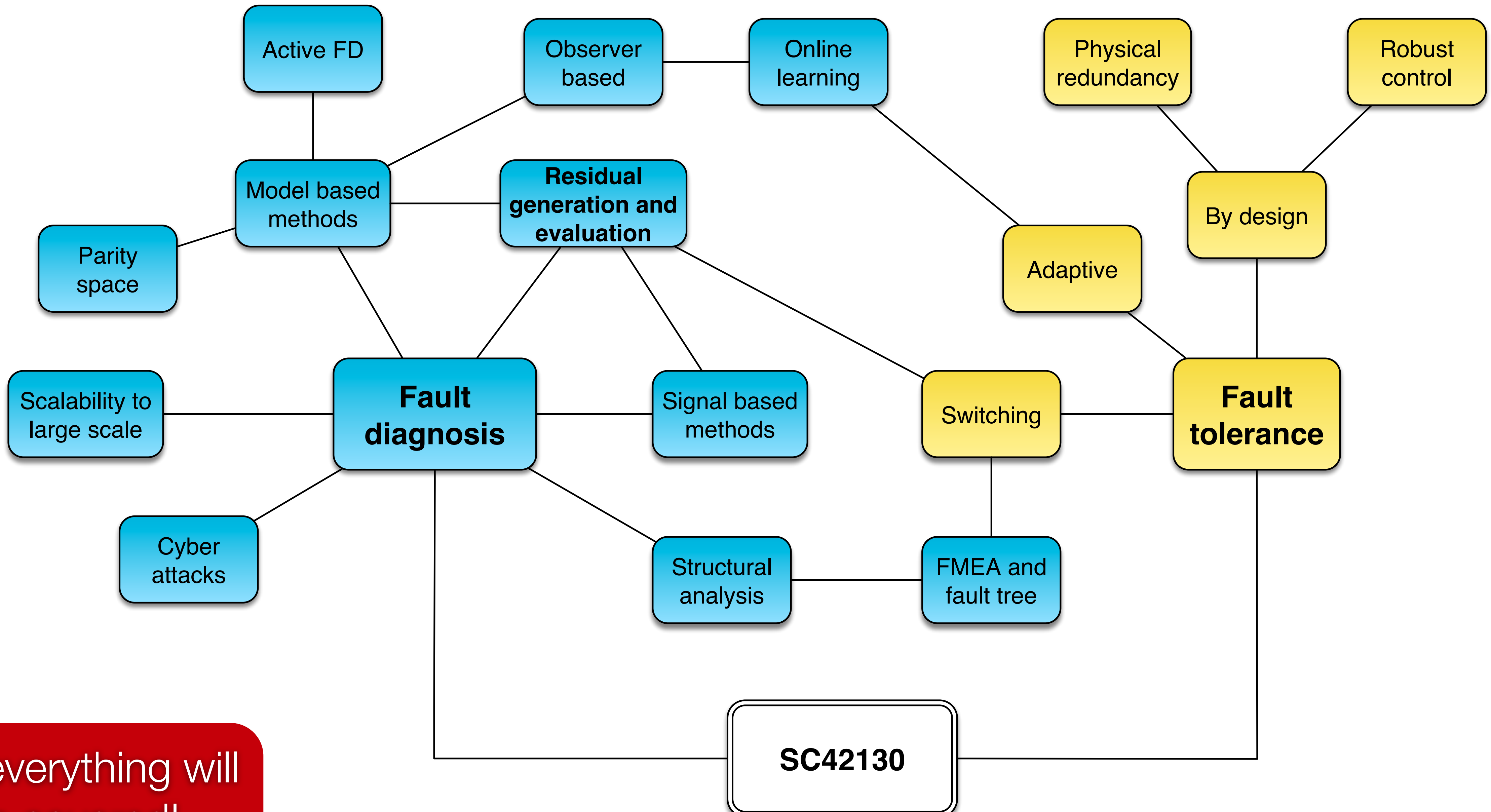
OPEN QUESTION

Pros and cons of different kind of redundancies?

	Hardware	Physical	Analytical
Pro	You can guarantee same level of performance	If you can afford it, it is the best	It is the most efficient (SW only)
Cons	• costly • What if switched in component is faulty too?	• Huge cost • Not always possible	• Cannot guarantee performance level

A VISUAL INTRODUCTION

A taxonomy of FD and FT



Not everything will be covered!

DEFINITIONS AND MODELS

Getting to know key terms and models

DEFINITIONS AND MODELS

Faults

> From [**BL06**]:

*"A **fault** in a dynamical system is a **deviation** of the system structure or the system parameters from the **nominal** situation",*

> From [**IS06**]:

*"A **fault** is an unpermitted **deviation** of at least one characteristic property (feature) of the system from the acceptable, usual, **standard** condition".*

[**BL06**] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault Tolerant Control*. Springer Verlag, 2006.
[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Failure

> From [**IS06**]:

*"A **failure** is a **permanent interruption** of a system's ability to **perform** a **required function** under specified operating conditions".*

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Failure

> From [**IS06**]:

*"A **failure** is a **permanent interruption** of a system's ability to **perform** a **required function** under specified operating conditions".*

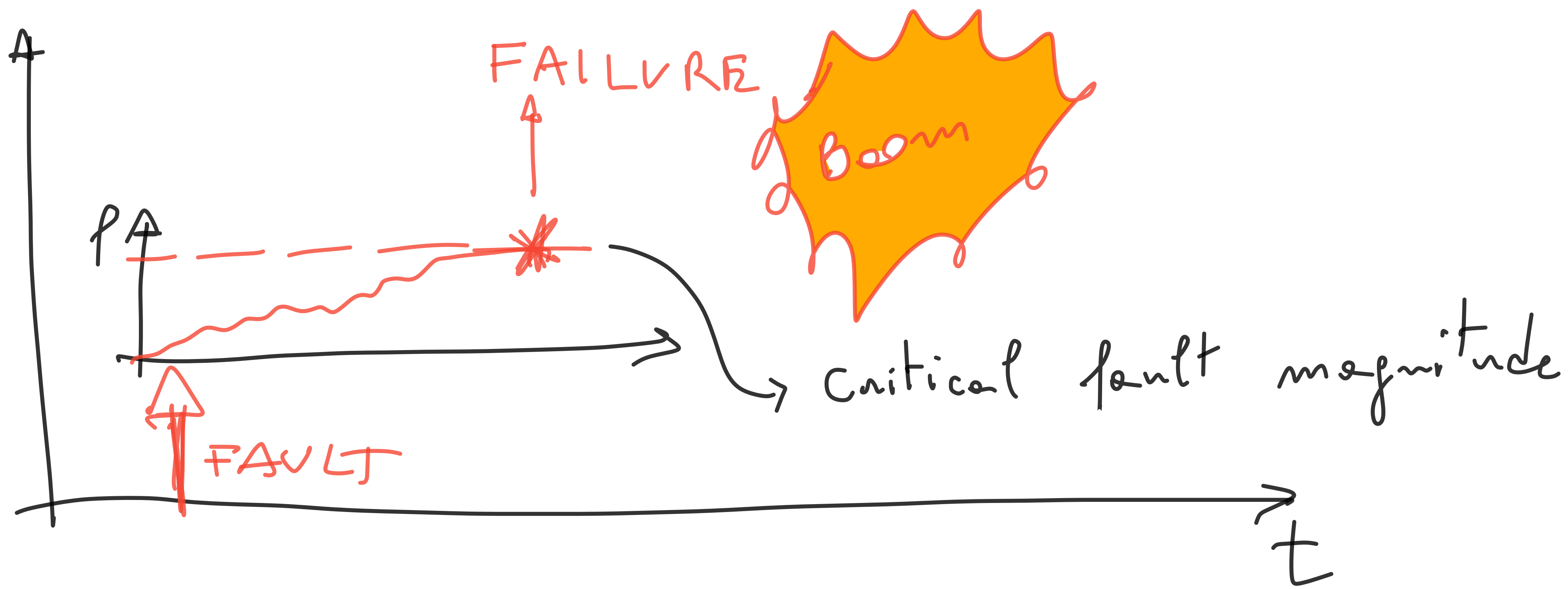
[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Failure

> From [**IS06**]:

*"A **failure** is a **permanent interruption** of a system's ability to **perform** a **required function** under specified operating conditions".*



[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Reliability

> From [**IS06**]:

*"**Ability** of a system to **perform** a required function under stated conditions, within a given scope, during a given period of time".*

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Reliability

> From [**IS06**]:

"***Ability*** *of a system to* ***perform*** *a required function under stated conditions, within a given scope, during a given period of time".*

Reliability ⇒ MTTF = $\frac{1}{\lambda}$ → Average # of failure per unite time

Mean Time To Failure

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Availability

> From [**IS06**]:

*"**Probability** that a system or equipment will **operate** satisfactorily and effectively at any period of time".*

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Availability

> From [**IS06**]:

*"**Probability** that a system or equipment will **operate** satisfactorily and effectively at any period of time".*

Availability $A = \dfrac{MTTF}{MTTF + MTTR}$

MTTR → Mean Time To Repair

$MTTR \downarrow \Rightarrow A \uparrow$

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Fault detection and fault diagnosis

> Adapted from [**IS06**]:

*"**Fault detection** consists in **determining** the **presence** of a **fault** in a given **system** at a given **time**"*

*"**Fault diagnosis** consists in **determining** the **presence**, **type**, **size** and **location** of a **fault** in a given **system** at a given **time**, assuming the **knowledge** of the **possible faults** affecting that given system"*

[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

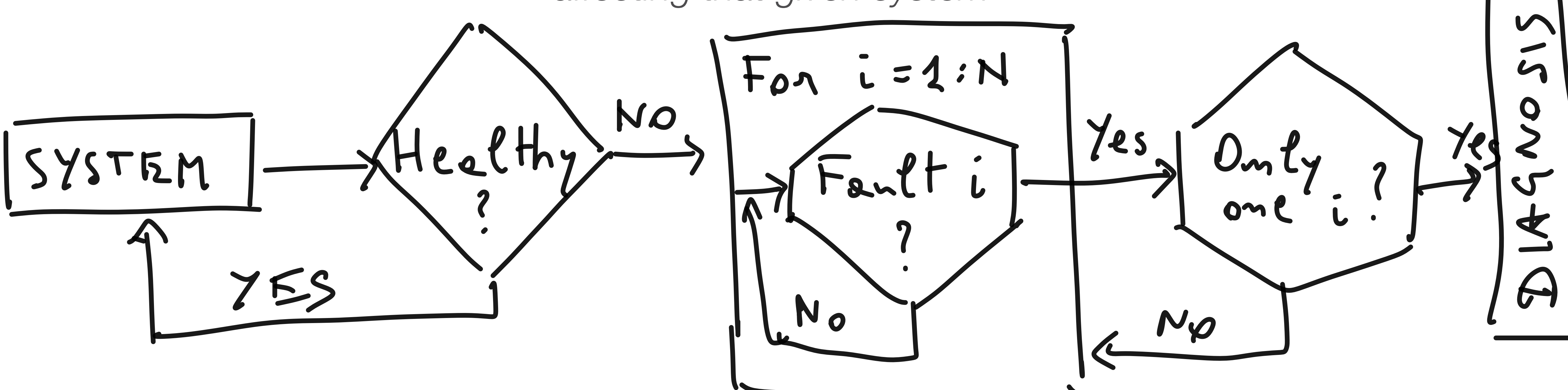
DEFINITIONS AND MODELS

Fault detection and fault diagnosis

> Adapted from [**IS06**]:

"***Fault detection*** *consists in* ***determining*** *the* ***presence*** *of a* ***fault*** *in a given* ***system*** *at a given* ***time***"

"***Fault diagnosis*** *consists in* ***determining*** *the* ***presence***, ***type***, ***size*** *and* ***location*** *of a* ***fault*** *in a given* ***system*** *at a given* ***time***, *assuming the* ***knowledge*** *of the* ***possible faults*** *affecting that given system*"



[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

DEFINITIONS AND MODELS

Fault tolerance

> From [**BL06**]:

"***Fault tolerance*** *is defined as the* ***possibility*** *of* ***achieving*** *a given (set of)* ***objective****(s) in the* ***presence*** *of a given (set of)* ***faults****".*

> From [**IS06**]:

"***[Fault] tolerance*** *describes the notion of trying to* ***contain*** *the* ***consequences*** *of* ***faults*** *and* ***failures*** *thus that the components* ***remain functional****".*

[**BL06**] M. Blanke, M. Kinnaert, J. Lunze, and M. Staroswiecki, *Diagnosis and Fault Tolerant Control*. Springer Verlag, 2006.
[**IS06**] R. Isermann, *Fault-diagnosis systems: an introduction from fault detection to fault tolerance*. Springer Science & Business Media, 2006.

OPEN QUESTION

What is *your* definition of fault tolerance?

DEFINITIONS AND MODELS

Nominal behaviour of a system

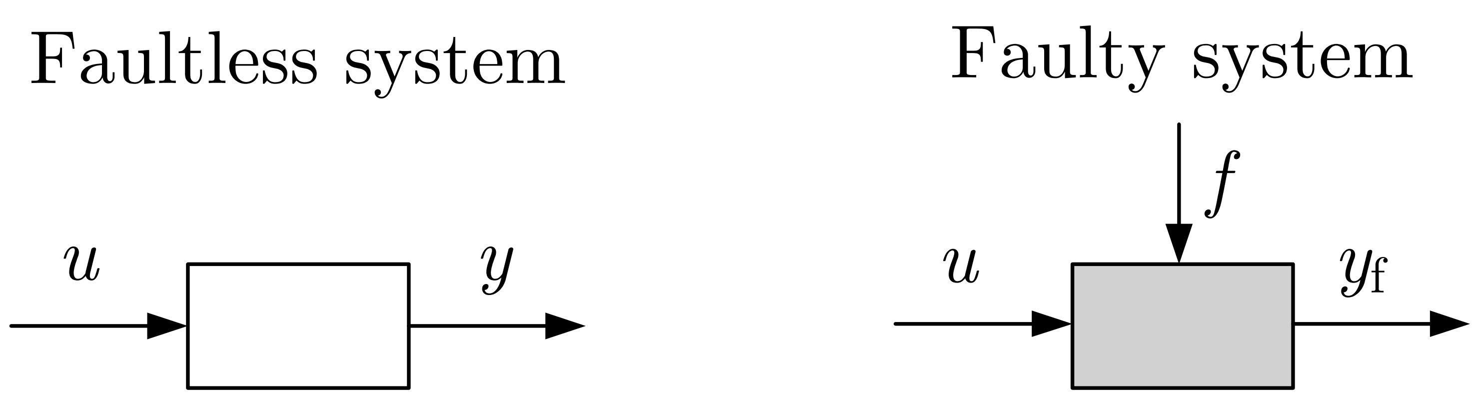
- All definitions of faults and failures refer to a nominal **condition**
- In our case (dynamical systems controlled in close loop) we prefer the term **behaviour**

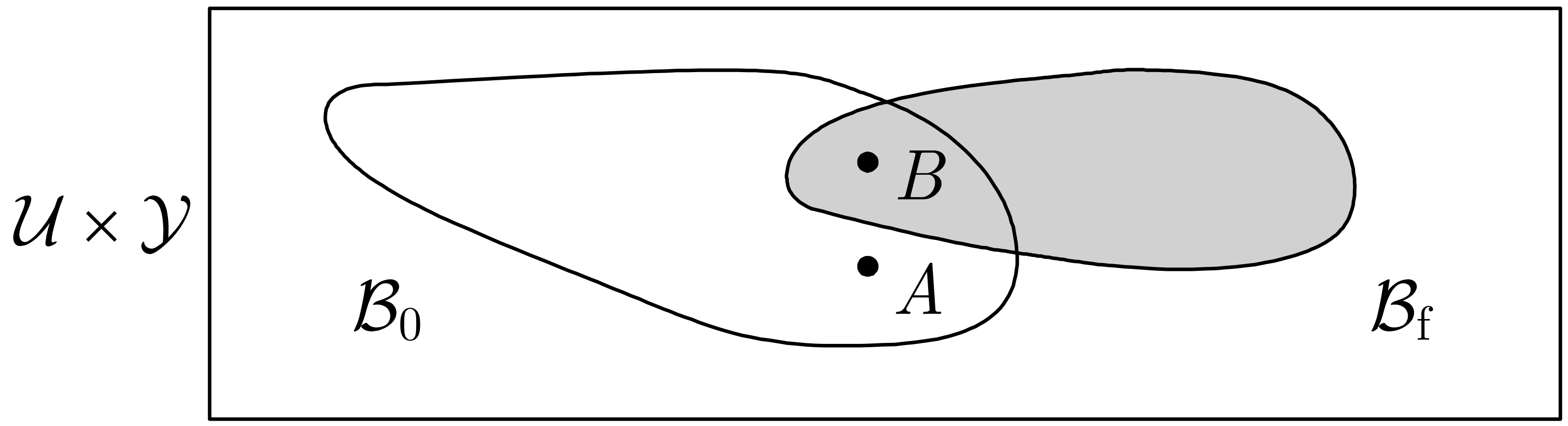
DEFINITIONS AND MODELS

Nominal behaviour of a system

> All definitions of faults and failures refer to a nominal **condition**

> In our case (dynamical systems controlled in close loop) we prefer the term **behaviour**



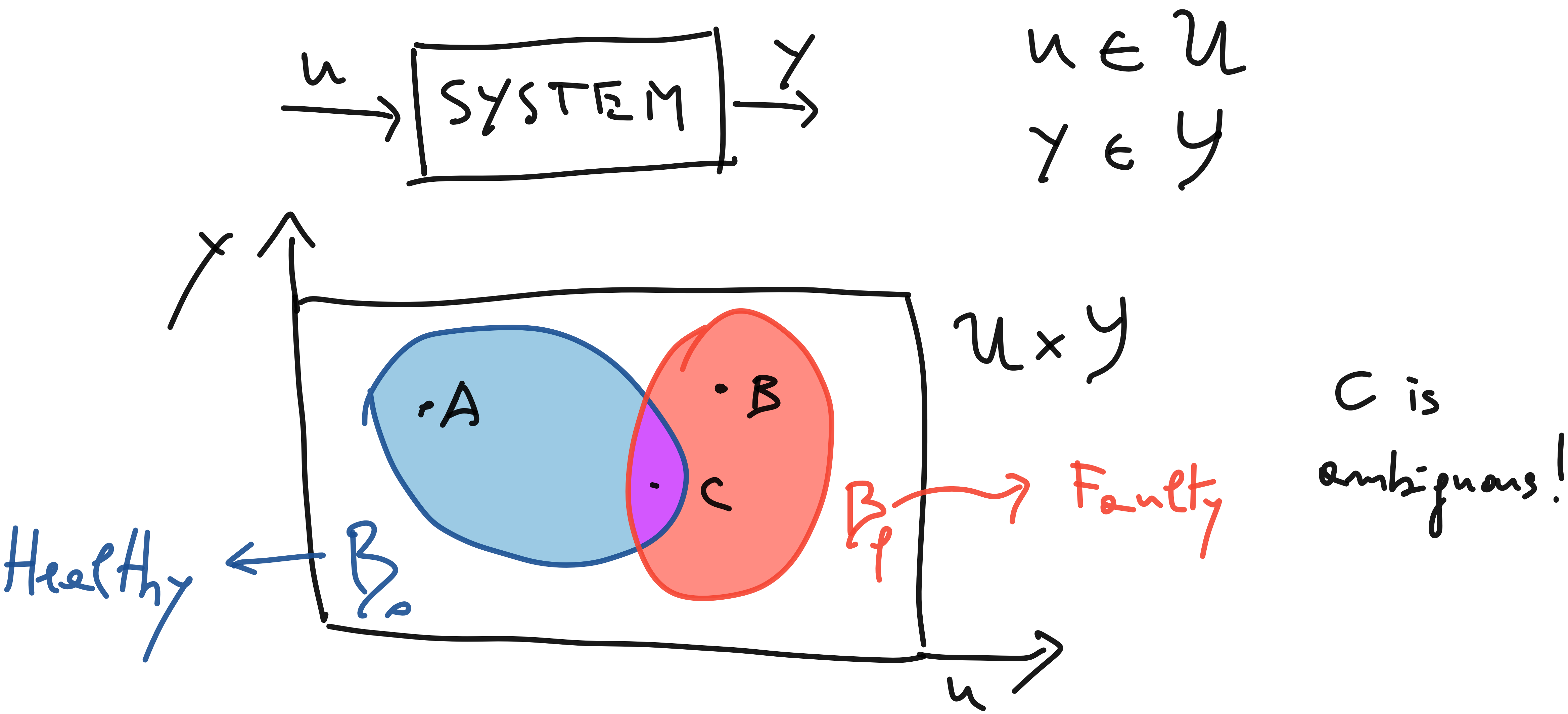


DEFINITIONS AND MODELS

Nominal behaviour of a system

> All definitions of faults and failures refer to a nominal **condition**

> In our case (dynamical systems controlled in close loop) we prefer the term **behaviour**



DEFINITIONS AND MODELS

Nominal behaviour of a system

> For dynamical systems, in general we use the following models

DEFINITIONS AND MODELS

Nominal behaviour of a system

> For dynamical systems, in general we use the following models

$$\begin{cases} \dot{x} = g(x, u, \underbrace{w}_{\text{uncertainty}}, \underbrace{f}_{\text{fault}}) \\ y = h(x, u, \underbrace{v}_{\text{uncertainty}}) \end{cases}$$

fault ($f = 0 \Rightarrow$ healthy)

uncertainty

Similarly in discrete time

QUESTION: Is this model general enough?
Can we represent all kind of faults?

FAULTS

A description of faults in dynamical systems

FAULTS

Time behaviour of faults

> How does the **magnitude** of a **fault** evolve?

Abrupt	Incipient	Intermittent

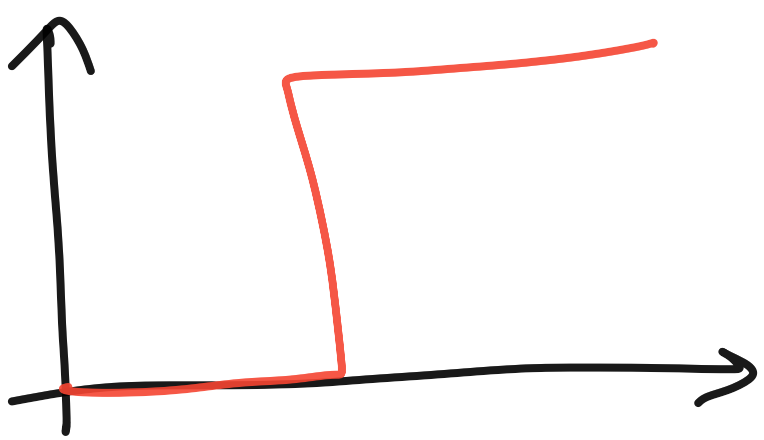
Note: **null** magnitude means **absence** of fault

FAULTS

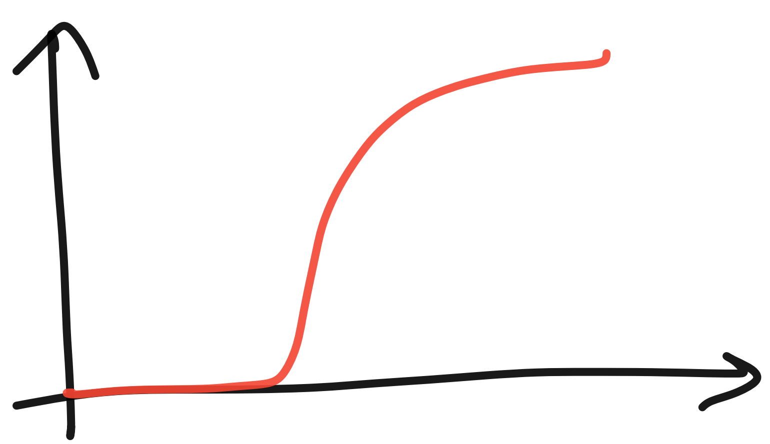
Time behaviour of faults

> How does the **magnitude** of a **fault** evolve?

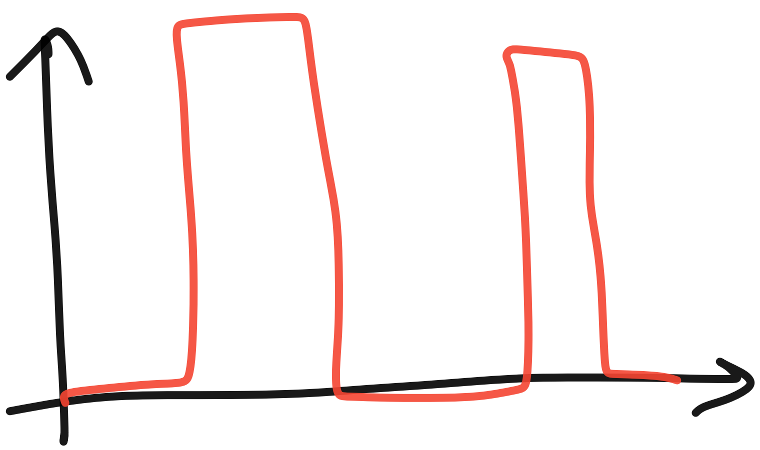
Abrupt



Incipient



Intermittent



Note: **null** magnitude means **absence** of fault

FAULTS

Location of faults

> Where does the **fault strike**?

Actuator	Plant	Sensor

FAULTS

Location of faults

> Where does the **fault strike**?

Actuator	Plant	Sensor
$\tilde{u} = u(1+f)$	$\dot{x} = \cancel{\tilde{g}}(\dots)$ Like g but for $f \neq 0$	$\tilde{y} = y + f$

FAULTS

Analytical model of faults

> How does a **fault** influence a dynamical system?

> Let us assume initially a **sensor** whose nominal output is $y(t)$

Additive	Multiplicative	General

FAULTS

Analytical model of faults

> How does a **fault** influence a dynamical system?

> Let us assume initially a **sensor** whose nominal output is $\boldsymbol{y(t)}$

Additive	Multiplicative	General
$\tilde{y} = y + f$	$\tilde{y} = y(1+f)$	$\tilde{y} = \varphi(y)$

CONCLUSION

Recap of this lecture and plan for next

- **THIS LECTURE**
  - We introduced **definitions** of key terms
  - We provided a **taxonomy** of faults and failures
- **NEXT**
  - **Introduction and taxonomy of FD and FT approaches**

CONCLUSION

Thank you for your attention !

For further information:

Course page on Brightspace

or

r.ferrari@tudelft.nl