

Historical changes in the concept of safety. A new approach for a modern society

Gilles MOTET
LAAS, Univ. Toulouse &
Foundation for an Industrial Safety Culture



Gilles.Motet@laas.fr
Gilles.Motet@foncsi.org



Introduction



② Professor at INSA Toulouse

② Software to System dependability:

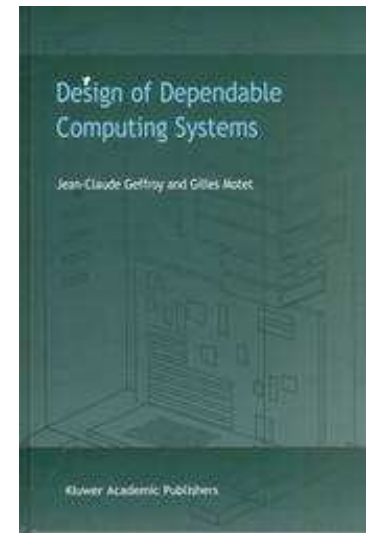
☆ Prentice Hall (1996), InterEditions (1998), Kluwer (2002)

② Safety to Risk Management

② Researcher at CNRS (LAAS)

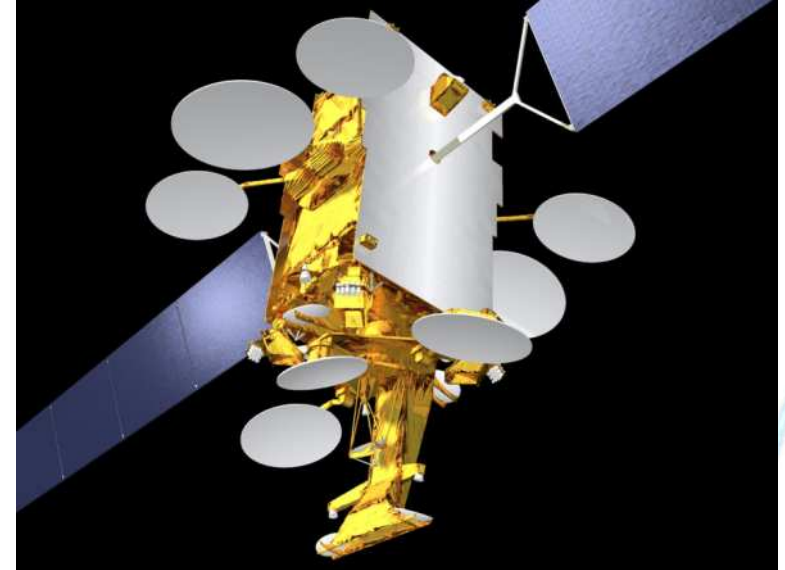
② ISO TC 262: “Risk Management”

② Scientific Director of the Foundation for an Industrial Safety Culture



Toulouse

Industries ...

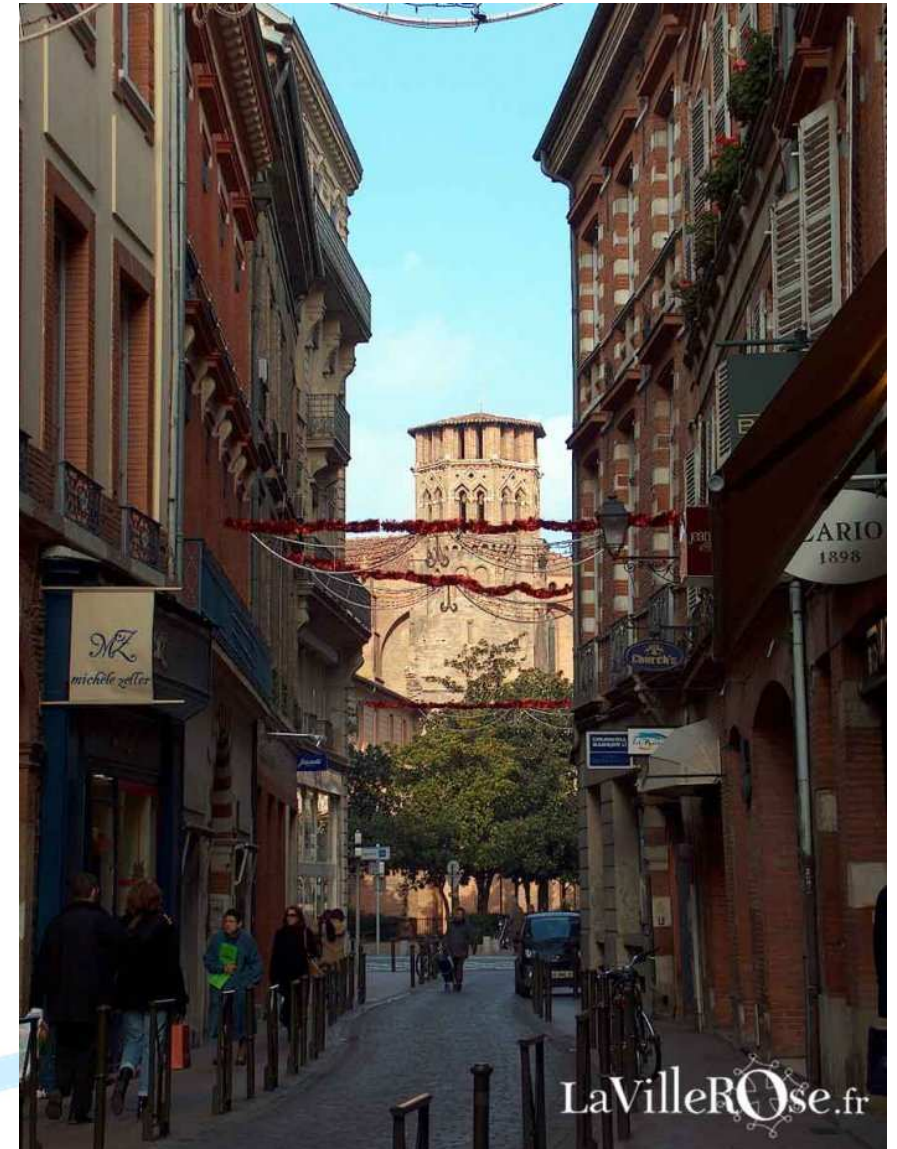


Best rugby team ...

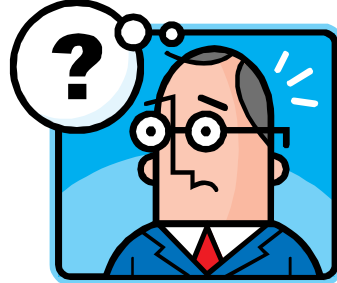


Toulouse

and a southern-european atmosphere

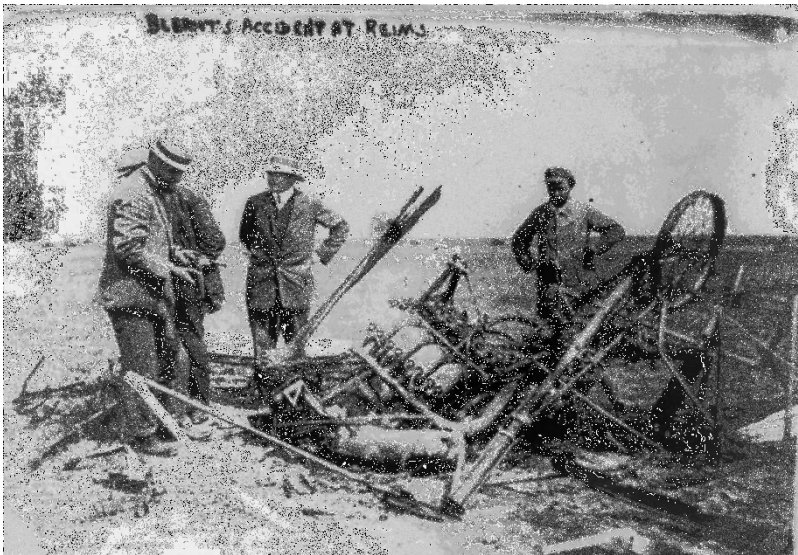


Presentation objectives

- ② Risk (safety) = combination of the probability of occurrence of harm and the severity of that harm (Guide 51, 1990, 1999, 2012)
- ② Risk = the effect of uncertainty on objectives (ISO 31000, 2009) 
- ② Risk & safety definitions changes resulting from societal changes
- ② Highlight effects on Mgt of safety by owners & regulators

Hazard (1st phase)

- ⌚ Risk = Hazardous phenomenon (hazard)
- ⌚ Energies: Potential, kinetic, thermal, etc.
- ⌚ Risk = a concept from Physics



- ⌚ Harms = “cost of progress”

Hazard

⌚ **Still frequently held viewpoint**

⌚ **Extended to**

- ☆ toxicity of products
- ☆ failure of system functions
- ☆ ...

⌚ **Negative and intrinsic**

- ☆ Laws of physics
- ☆ Close to “natural risk”

Hazard

- ⌚ Stakeholders define **Safety** relative to the absence of hazard
 - ☆ “**Situation without hazard**”
 - ☆ “Peace of mind resulting from the absence of hazard”
- ⌚ **Regulators require hazard elimination**
 - ☆ 1893: cars banned in Nice city center
 - ☆ 2011: shale gas drilling banned in France

Hazard

⌚ Risk = Hazard

★ Hazard analysis



Hazardous
Phenomenon

★ Treatment = elimination / reduction

- ➔ Reduction of the negative effects
- ➔ **As well as the benefits**

★ E.g. High altitude of aircraft allows

- ➔ Fuel consumption reduction
- ➔ Reduction of emissions and ticket cost

Hazard

☆ How to balance Safety & Benefits?
=> Not negociable

→ "Safety first"! ->



⊙ These [hazardous] phenomena may increase safety

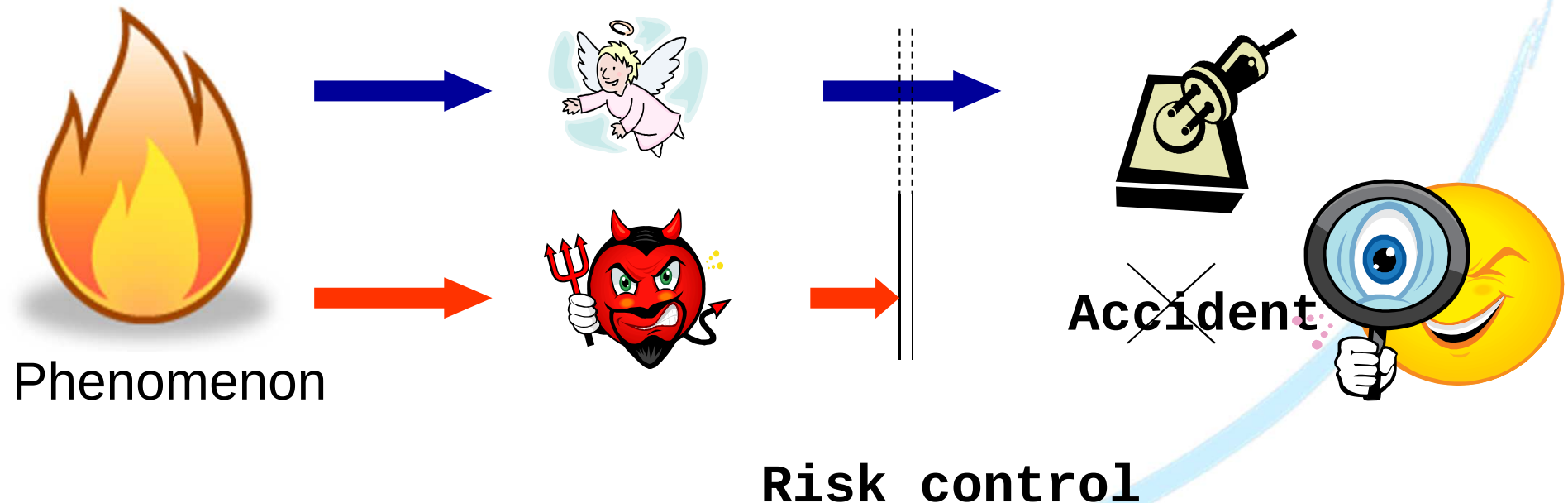
- ☆ speed reduces falls (gyroscopic effect)
- ☆ leaning increases potential energy & safety



Harmful event (2nd phase)

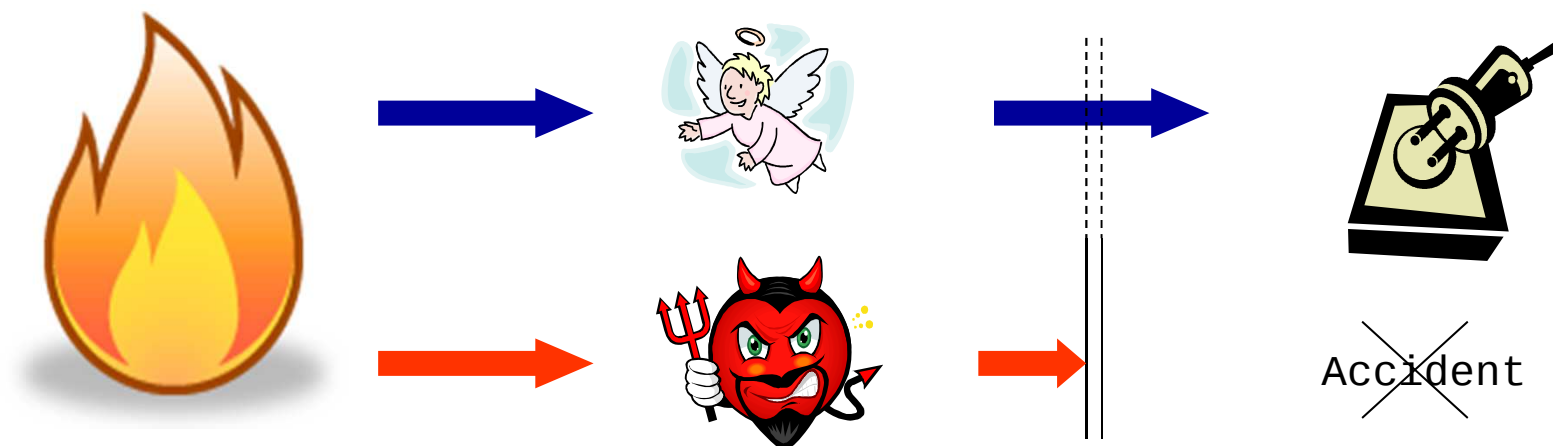
⊙ **Risk = Potential harmful event**

☆ Avoidance of the **negative effects**
(not the phenomenon)



Harmful event

- ⊙ **Safety = Absence of accident**
(before: *absence of hazards*)



Phenomenon

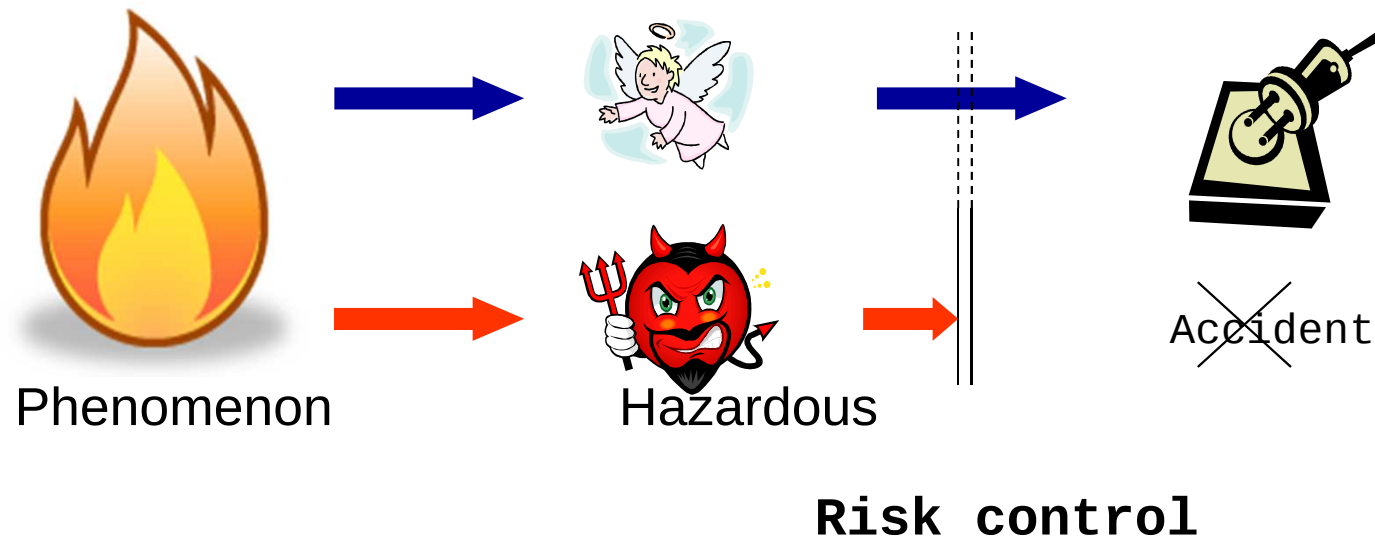
Hazardous

Risk control

☆ From *physical* to *abstract* viewpoint
(event)

Harmful event

⌚ Safety = Absence of accident



★ Risk assessment

- ➡ (1) based on the past (« Peace of mind resulting from the *absence of accident* »)
- ➡ (2) Assumes deterministic cause to effect relationship (physical law)

Harmful event

⌚ Safety = Absence of accident

☆ Absolute concept: true or false

☆ In reality same circumstances $\neq$ same effects

⌚ Safety = “Freedom from *unacceptable* risk” (Guide 51, 1999)

⌚ Safety = relative concept

Harmful event

② Which risk criteria to define the social acceptability of risk?

1. Likelihood of accident $<$ Threshold

☆ Accident:

from *impossible* to *improbable*

☆ To control (vs. prohibit) accident occurrences

☆ Assessment: Probabilistic approaches

Harmful event

2. Integration of consequences

⌚ Risk = combination of the probability of occurrence of harm and the severity of that harm (Guide 51, 1999)

⌚ Ex. Avionics regulation:
 $\text{Prob}(\text{Crash}) < 10^{-9}/H$

⌚ Risk is

☆ More abstract: $\varphi \rightarrow \text{Evt} \rightarrow \text{Potential evt}$

☆ Negative

Acceptable $\neq$ Desirable



Unacceptable

Harmful event

3. Regulator compares individual harms with collective benefits

☆ Bernouilli, 1760: vaccination of variola

⇒ fatal for certain persons, but

⇒ Overall life expectancy increase: 3 years

☆ **Risk = combination of an event and its consequences (Guide 73, 2002)**

☆ **Risk = neutral concept / objectives**

What does risk acceptability mean?

@ If $P(\text{Crash}) < 10^{-9}/H$ is acceptable risk

☆ Why do stakeholders hesitate to fly after an crash?

☆ Why does the regulator require a design change?

☆ Why can airlines be sued (society)?

What does risk acceptability mean?

@ Is **Probability(Crash) $< 10^{-9}/H$**

☆ An acceptable quota?

➔ The estimated cost to be paid for progress

☆ A killing permit for engineers?

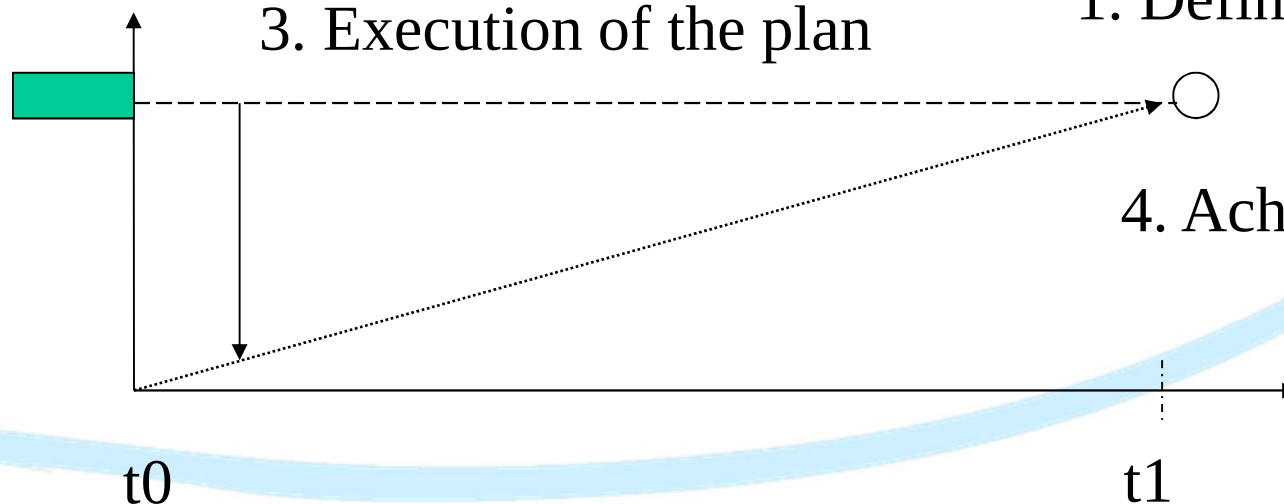
➔ To take into account economic requirements?

Effect of uncertainty (3rd phase)

② Engineers aim at zero accidents = their objectives (they do their best):

- ☆ Safety margins, Redundancies
- ☆ Fail-safe
- ☆ Maintenance
- ☆ Pilot

2. Action plan

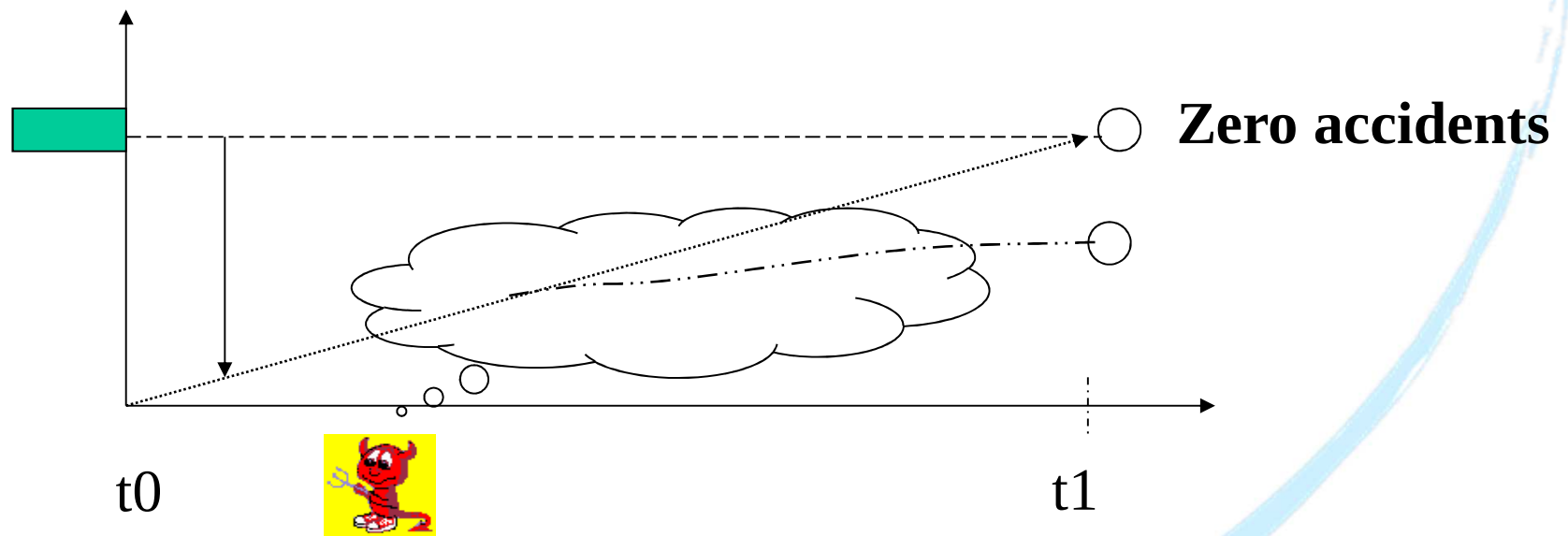


Effect of uncertainty

But engineers are faced with *uncertainty*

Limited knowledge, imperfect models, limited analysis tools,
human errors, etc.

They do the best *they can*



**Risk (*ISO 31000 / 2009*) = effect of uncertainty on
[the achievement of] the objectives**

Uncertainty handling

⌚ How to handle uncertainty?

- ☆ Suppressing uncertainty?

- ☆ Prohibiting its negative effects?

- ☆ Controlling its negative effects?

⌚ Is uncertainty the new hazard?

Uncertainty handling

② **Uncertainty cannot be suppressed by knowledge**

☆ More science => New questions!

② **Uncertainty is intrinsic to nature & physical phenomena**

☆ Natural risk (earthquakes, etc.) & probabilistic laws

Uncertainty handling

② Uncertainty provides benefits

- ☆ **Scientific discovery:** Penicillin by Alexander Fleming (1928)

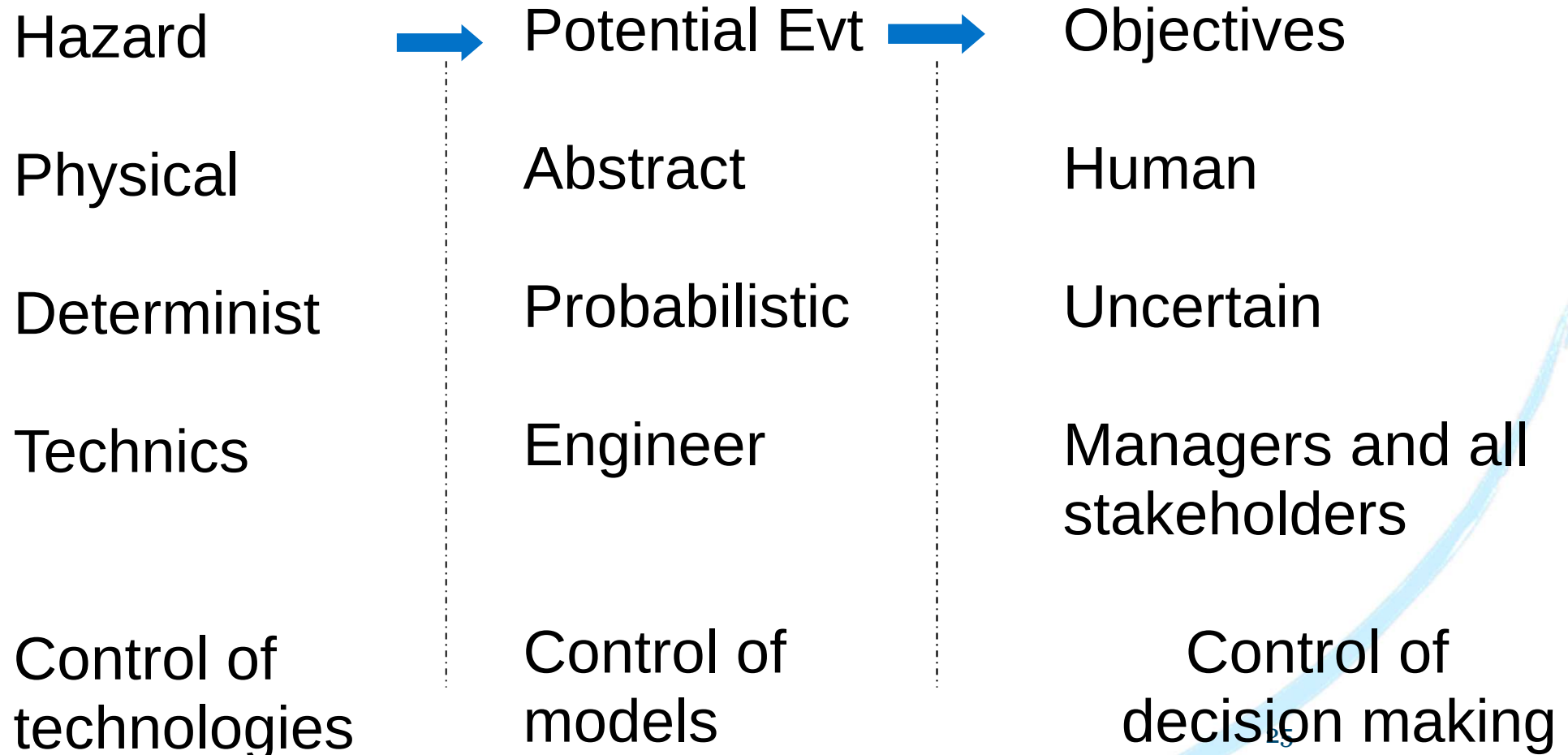
- ☆ **Allows decision-making**

② is not the new hazard to be avoided

② is a phenomenon whose effects have to be controlled

Uncertainty: A new challenge for safety

Three steps:



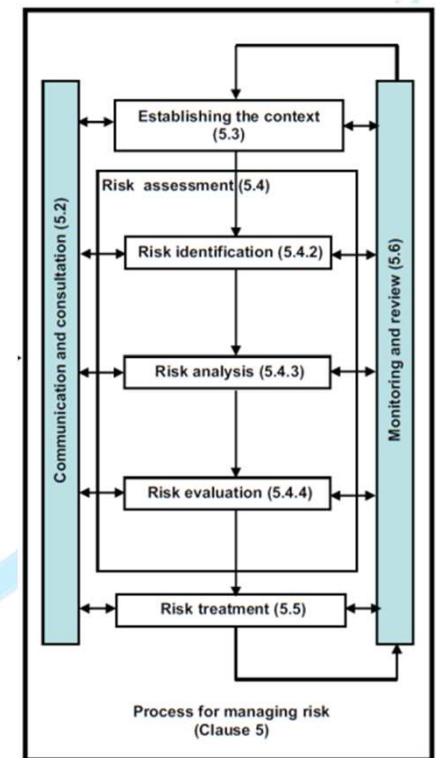
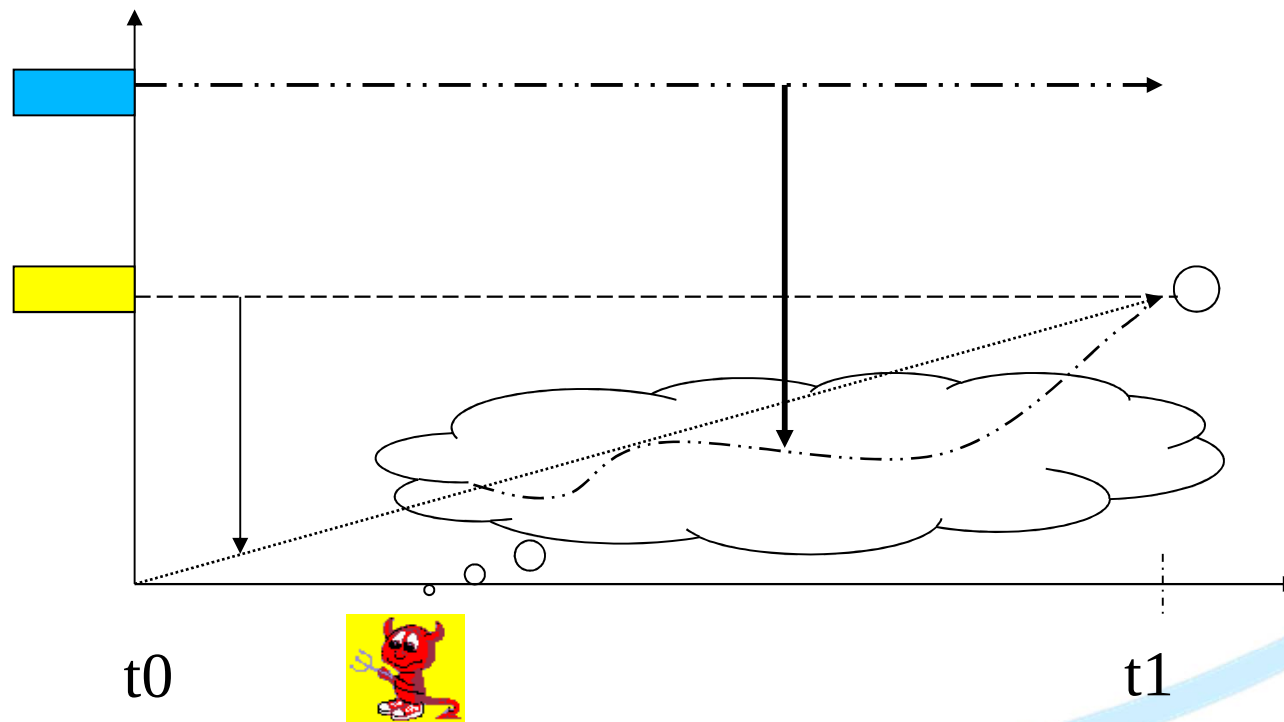
How to deal with this new challenge?

Risk Management Process

@ Two planned activities at t_0 :

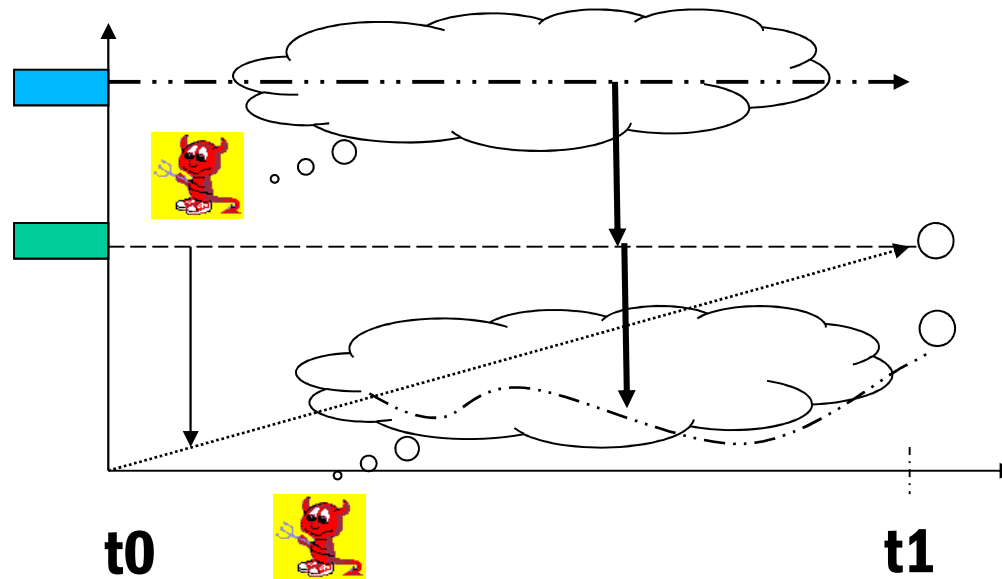
☆ Activity to achieve objectives 

☆ RM activity to control risks 



Risk Management Process

- ② Uncertainty also affects activities of Risk Management process

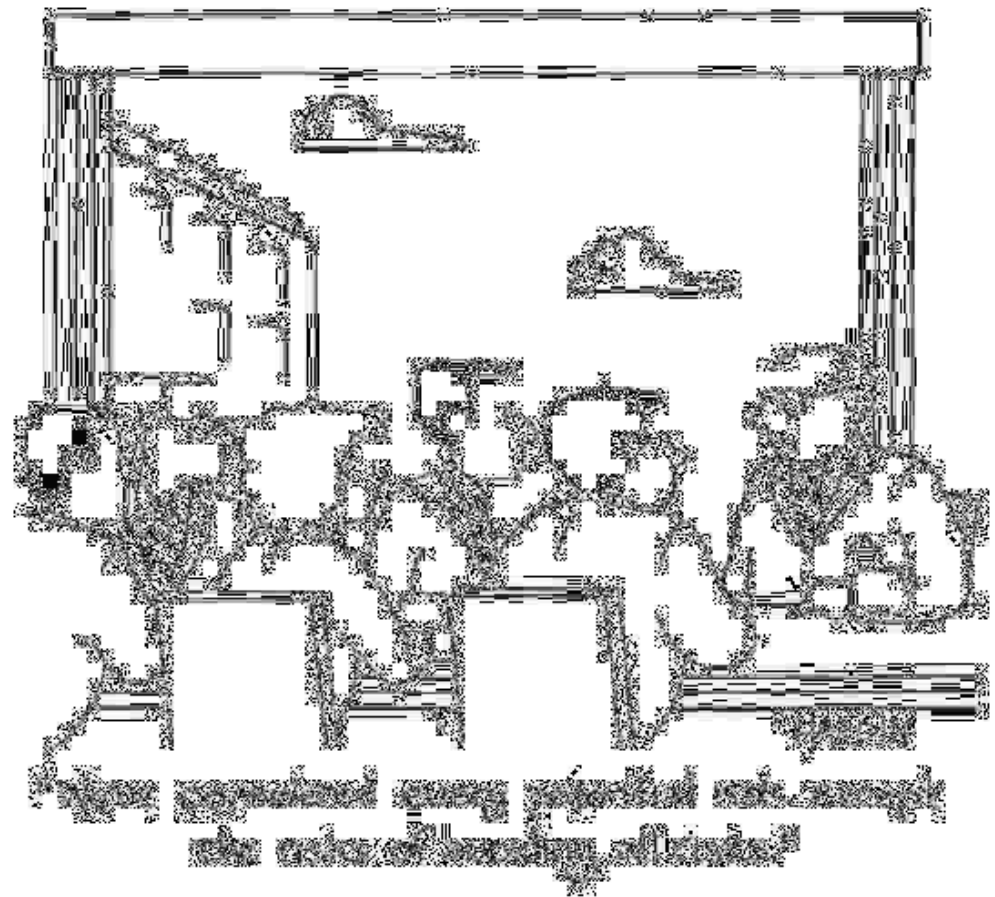
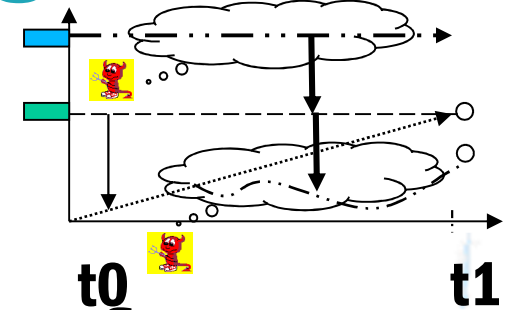


- ② Risk affecting risk management process

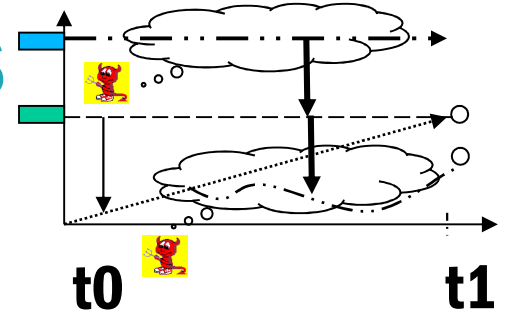
Risk Management Process

④ Examples of RM uncertainties

☆ Uncertainty of the completeness of identified risks



Risk Management Process



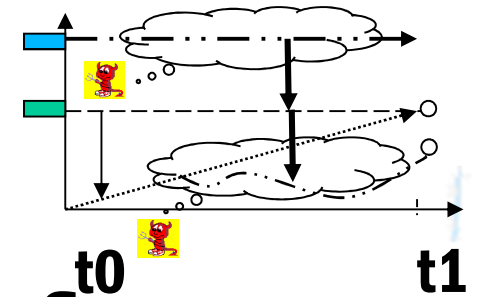
@ Examples of RM uncertainties

☆ Uncertainty on the selection and use of the analysis techniques
e.g. 31 methods in ISO 31010

☆ Uncertainty on the effectiveness of the controls
e.g. Rio-Paris crash: previous recoveries of sensor failures

☆ $10^{-9}/H$ = Measurement of the effect of uncertainty on achievement of Risk Management objectives

Risk Management Process



- ② How to control the effects of uncertainty affecting the risk Management process, that is, the risks of the RM activities?
- ② 1st question: What are the objectives of RM?
- ② Defined by the *Principles* of ISO 31000

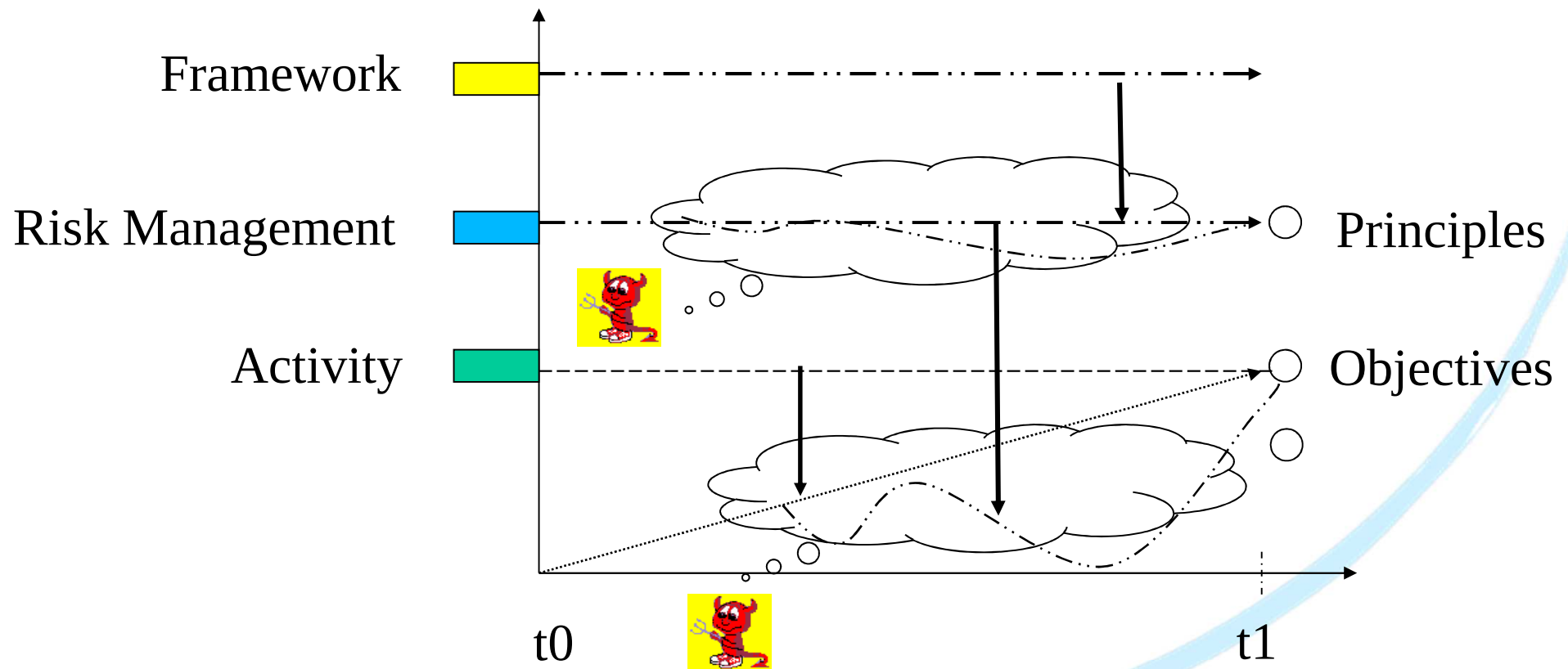
Principles

@ 1st Principle

- ★ **Risk Management should create value**
(useful to organisation objectives)
- ★ Uncertainty on RM usefulness
e.g. Bureaucratic activities
- ★ How to assess RM effectiveness
(leading indicators)?
- ★ How to improve RM effectiveness?
- ★ That is, **how to control the risks affecting RM activities relative to this 1st objective?**

Framework & Principles

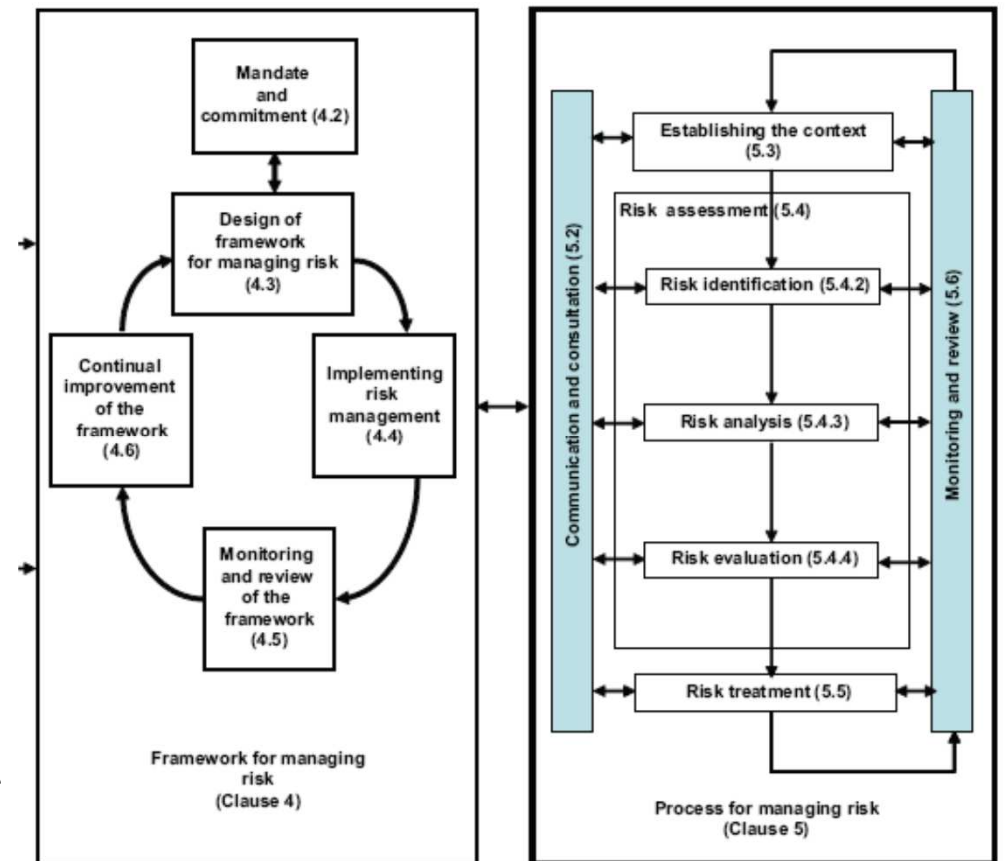
⌚ Framework = Process for handling effects of uncertainties on RM



Framework & Principles

② Framework = Process proposed by ISO 31000

② Hypothesis:
Uncertain RM is only accepted if it is continuously improved (PDCA) => *Best effort to achieve Principles*



Conclusion

@ Owners & authorities

- ☆ Have invested in RM process
- ☆ Should invest in the Framework
- ☆ Should audit their RM process to identify uncertainties which can affect the achievement of the Principles.

Thank you for your attention

Gilles Motet

Gilles.Motet@insa-toulouse.fr

Gilles.Motet@icsi-eu.org

Gilles.Motet@foncsi.org