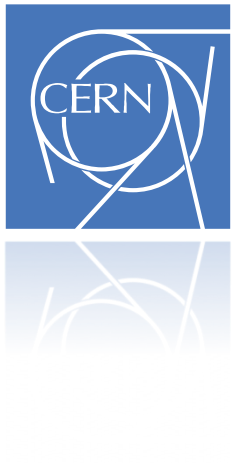


Organisation Européenne pour la Recherche Nucléaire
European Organization for Nuclear Research
Laboratoire Européen pour la Physique des Particules
European Laboratory for Particle Physics

How to include safety in a design study?

Pierre Bonnal
CERN DG-DI – Office of the Director for Accelerators and Technology

1st EUROnu Safety Workshop
Thursday 9th & Friday 10th June 2011
CERN, Geneva, Switzerland

Agenda

- Why including safety in a design study
- Safety documentation along the lifecycle of the facility, from design to dismantling
- Typical content of a Preliminary Safety Report

What is a successful project?

- Deliverable delivered, i.e. a facility delivered
  Performance achieved
  Good *if there is something!*

- No impact on persons, no accident
  No impact on the environment
  Bad *if there is something!*
  Corollary: ***Good*** *if there is nothing!*

What is a successful project? Trade-off

- Invest time & money for scientific performance

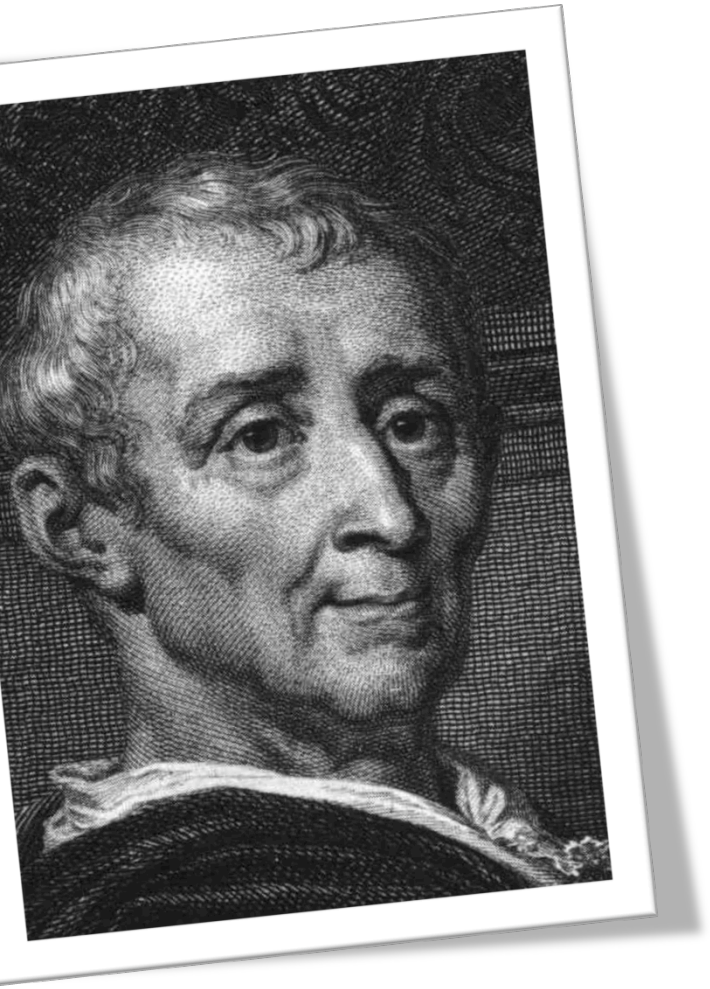
  Up to which amount? *"The more the better!"*

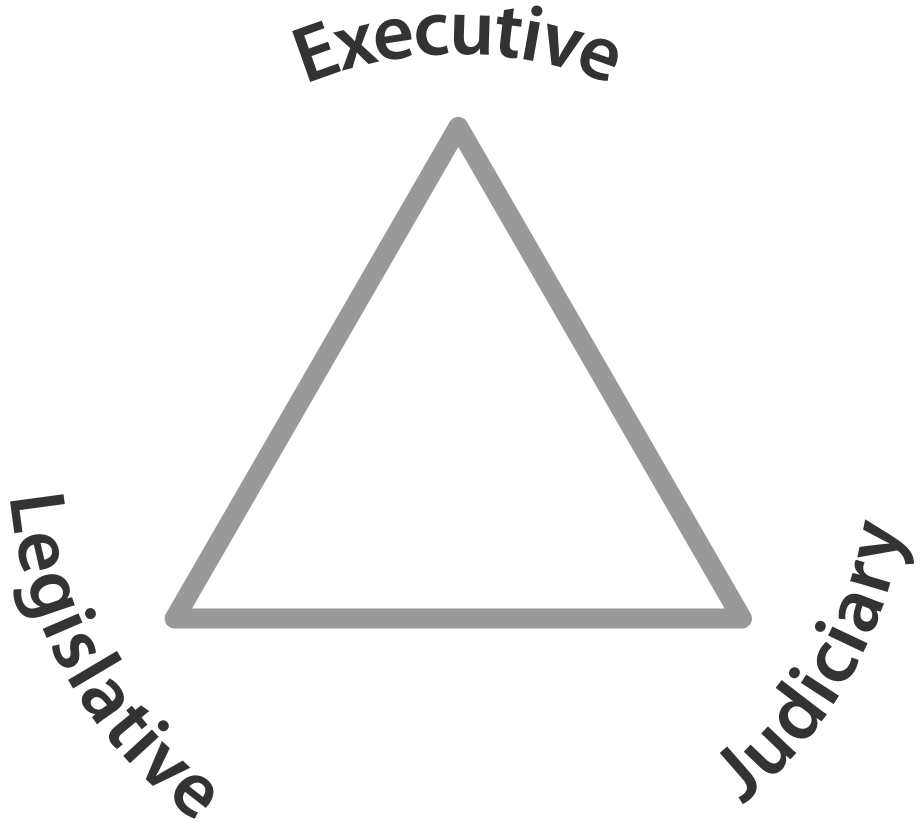
- Invest time & money for safety & environment

  Up to which amount? *"The more the better?"*

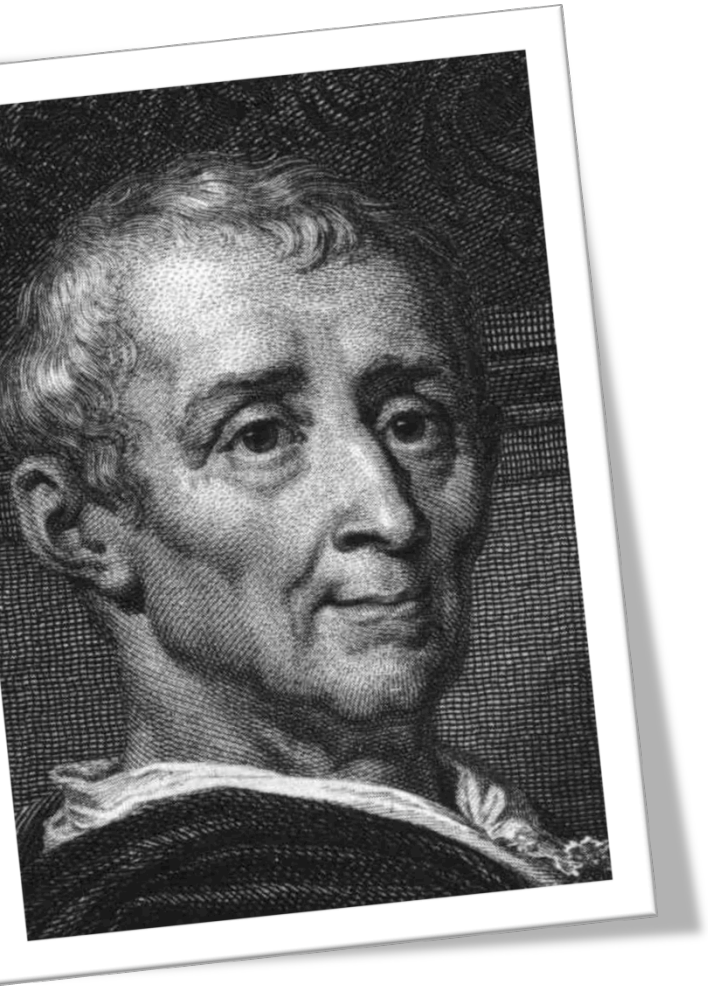
Some oversight is needed to insure that
a sufficient effort is made on safety aspects!

Montesquieu *The spirit of the laws* 18th century





Montesquieu *The spirit of the laws* 18th century



Executive

Study team then
Project team then
Operations team

Legislative

Safety regulations

Judiciary

Licensing authority

Some questions

1. Which safety regulations?
   - Different countries, different **approaches**
   - Different countries, different **regulations**
   - **Language** (not necessarily in English)
   - Nuclear safety regulations **limitations**
     (Nuclear Fusion Power Stations, Medical, Nuclear Weapons…)
   - Nuclear safety regulations **paradigm**
2. Which licensing authority?
   - Different countries, different **licensing authorities**

Montesquieu *The spirit of the laws* 18th century

Demonstration, by the Team
to the Licensing authority
that the Regulations are fulfilled

Two perspectives

- The facility should not injure worker/people nor release effluents in the environment
  to do so: **it should operate reliably**
  - Facility integrity, Nuclear safety, *Sûreté*

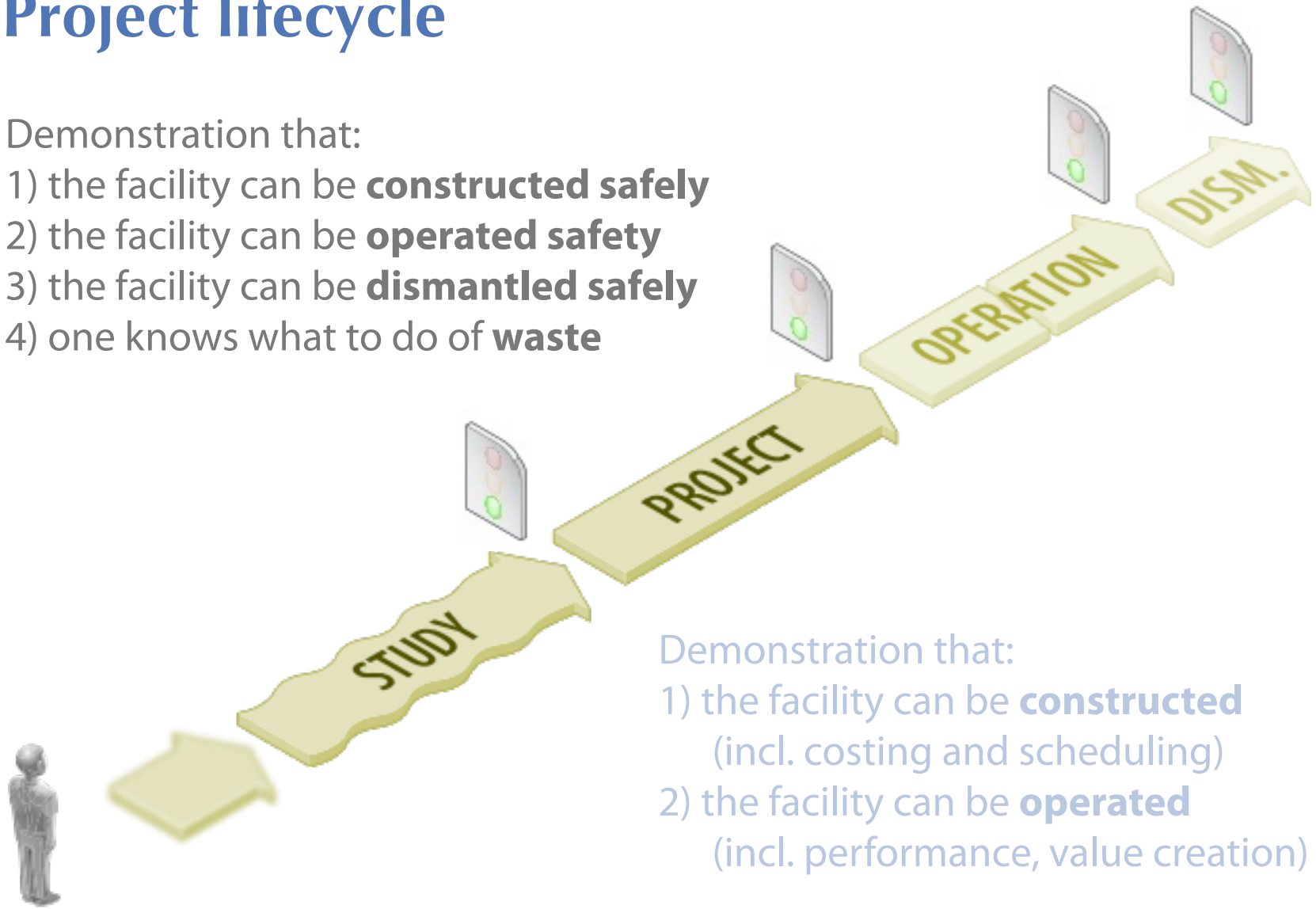
- Workers should not be injured by the facility
  - Occupational / health safety,
    Radiation protection, *Sécurité*

Montesquieu *The spirit of the laws* 18th century

Demonstration, by the Team
to the Licensing authority
that the Regulations are fulfilled,
from the 2 perspectives:
integrity and safety

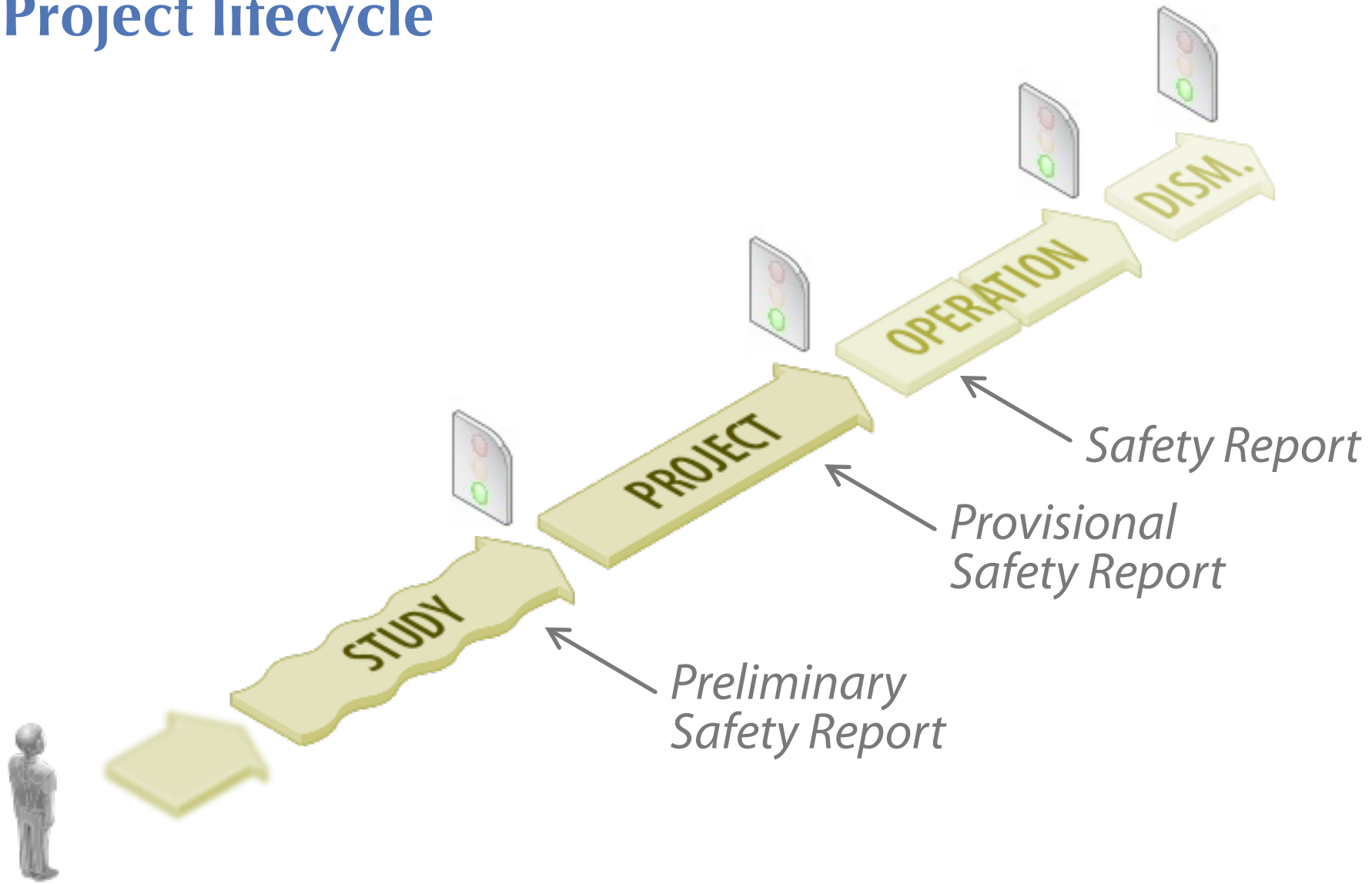
Project lifecycle

Demonstration that:
1) the facility can be **constructed safely**
2) the facility can be **operated safety**
3) the facility can be **dismantled safely**
4) one knows what to do of **waste**



Demonstration that:
1) the facility can be **constructed**
(incl. costing and scheduling)
2) the facility can be **operated**
(incl. performance, value creation)

Project lifecycle

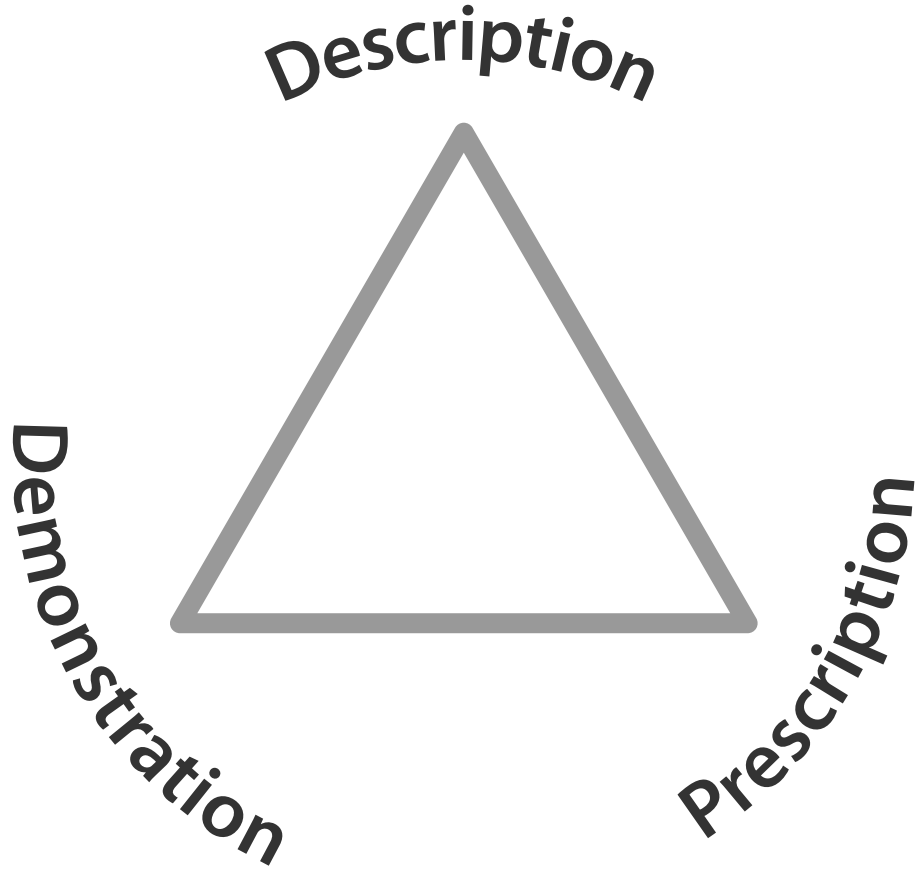


Principle

« *Un document ne vaut que quand on sait à qui il s'adresse* »

The value of a document depends on whom it is prepared for

Safety reports



Safety reports 1. Descriptive part

- Description of the facility/process
  - Why is it useful
  - Where is it located
  - What is it made of
  - How does it work
  - When will it be constructed, operated, dismantled
  - Who is responsible for its construction…
  - With which means will it be constructed…

« Quis, Quid, Ubi, Quibus auxiliis, Cur, Quomodo, Quando »

- Which **hazards** is present in the facility/process?

Safety reports 2. Demonstrative part

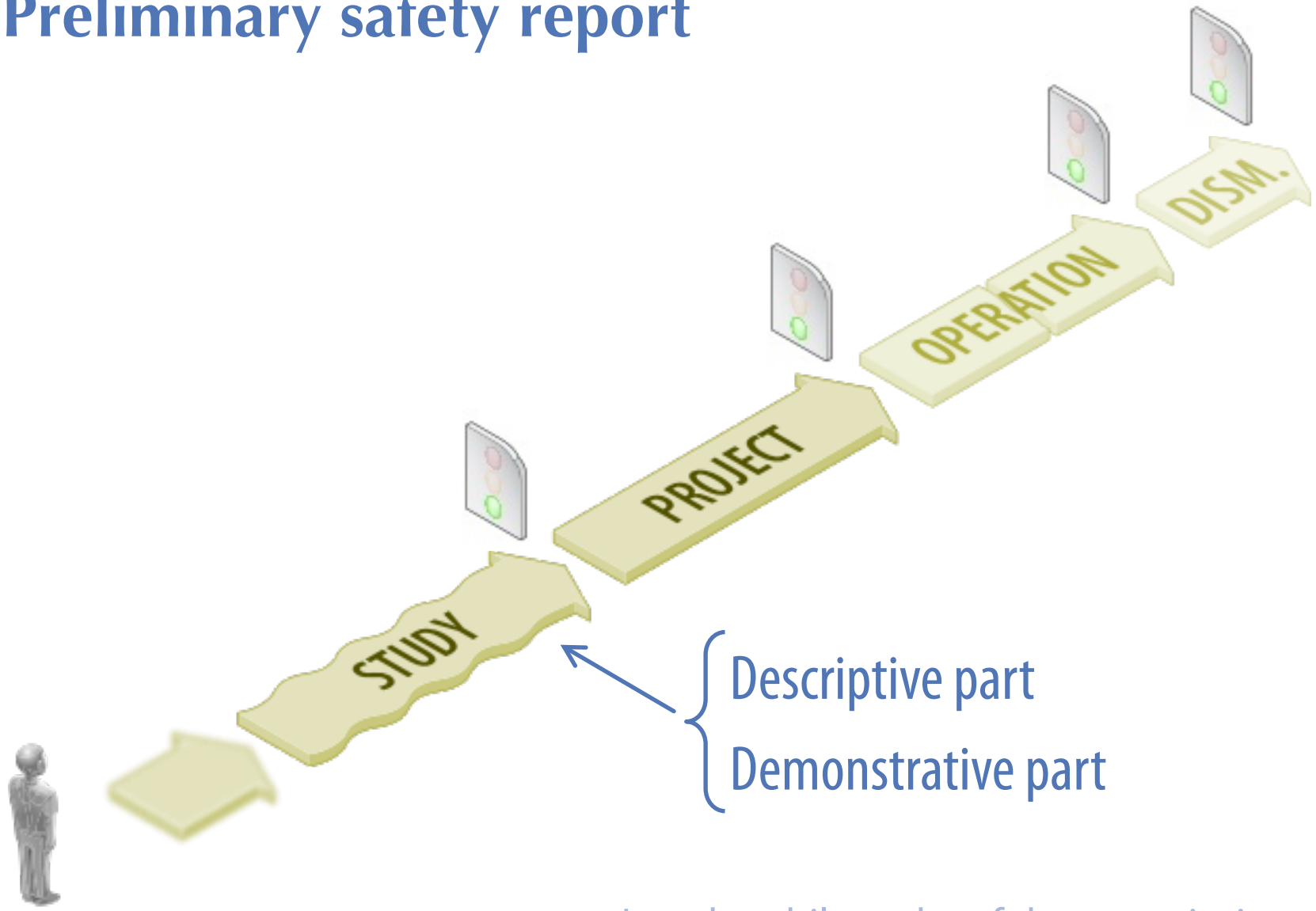
- Hazard/risk identification
- Risk evaluation
- Risk analyses
- Risk responses/treatments

Impact study

Safety reports 3. Prescriptive part

- Operations boundaries
  - operations thresholds not to overcome
- Organizational structures
  - for handling the project, constructing the facility
  - for operating and maintaining the facility
  - for dismantling the facility and handling waste
- Operations instructions and procedures
  - for operating the facility
  - for maintaining and ensuring its integrity
- Quality management framework

Preliminary safety report



Just the philosophy of the prescriptive part

Preliminary safety reports Descriptive part

- Description of the facility and of the process

  « Quis, Quid, Ubi, Quibus auxiliis, Cur, Quomodo, Quando »

- Which **hazards** are present in the facility/process?
  - Energy and radiological source terms
  - External (environmental) hazards
  - Internal (processes/utilities) hazards

  Identification:
  - Vade mecum, knowledge sharing…
  - Systematic approaches (process/utility diagrams, layouts)
- **Safety philosophy** (incl. applicable regulations…)

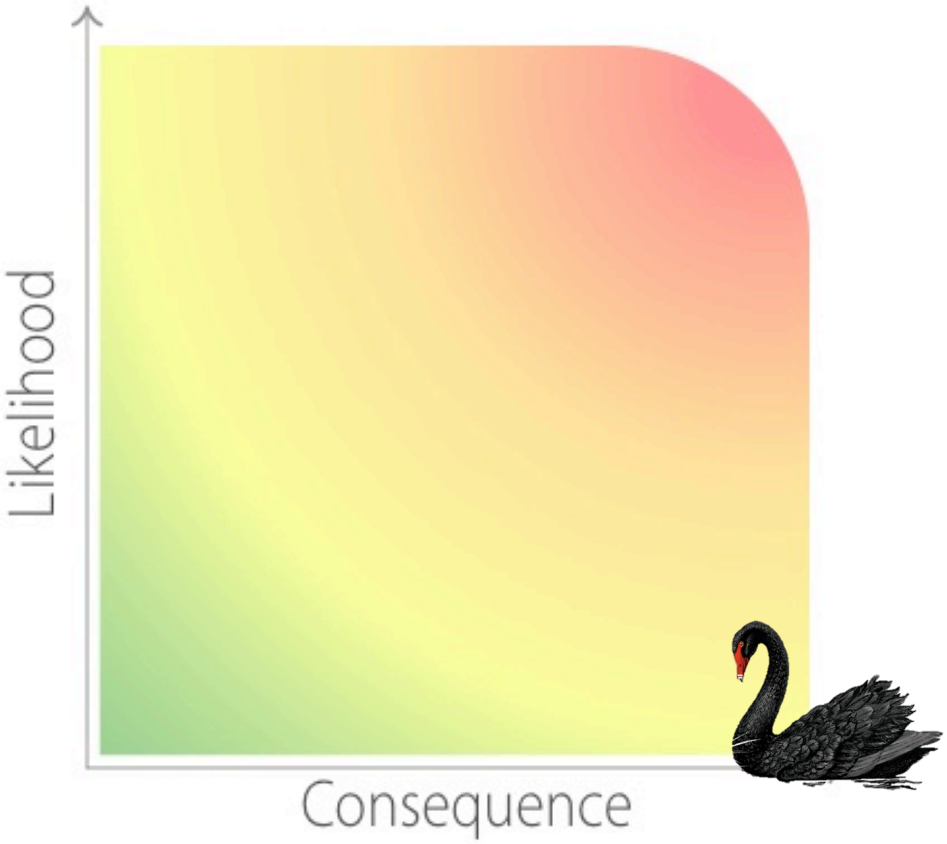
Preliminary safety reports Demonstrative part (1/2)

- Risk identification (see hazard identification)
  - Sequence of events
  - Potential incidental/accidental situations
- Risk evaluation
  - Risk assessment matrix

    $$\text{risk level} = \text{likelihood} \times \text{consequence}$$
  - Failure mode and effects analysis (FMEA)

    $$\text{severity} = \text{probability} \times \text{detectability} \times \text{gravity}$$
- Risk analyses

Risk evaluation



Risk evaluation Likelihood

Level	Justification
LOW Likelihood	Very unlikely because: → never happened, or already happened but over the last 10 years, or → has already happened (we heard of) in other organizations, but over the last 5 years, or → major catastrophe independent of our activities (e.g. earthquake).
MEDIUM Likelihood	Likely, may happen sometimes: → already happened within the last 10 years, or → already happened in other organizations within the last 5 years.
HIGH Likelihood	Very likely, may occur repetitively: → happened at least once for one-of-a-kind (project) activities → happened at least once per year for recurring activities.

Risk evaluation Consequence

Level	Justification
LOW Environmental and Safety Consequence	**Marginal:** → Releases constrained within our premises, or → Light injury requiring medical attention; no loss of working day.
MEDIUM Environmental and Safety Consequence	**Significant:** → Releases outside the our premises, easily remediable, or → Extensive injury; loss of working days.
HIGH Environmental and Safety Consequence	**Critical** or **catastrophic:** → Releases outside the our premises, hardly remediable, or → Injury with permanent disability; loss of life.

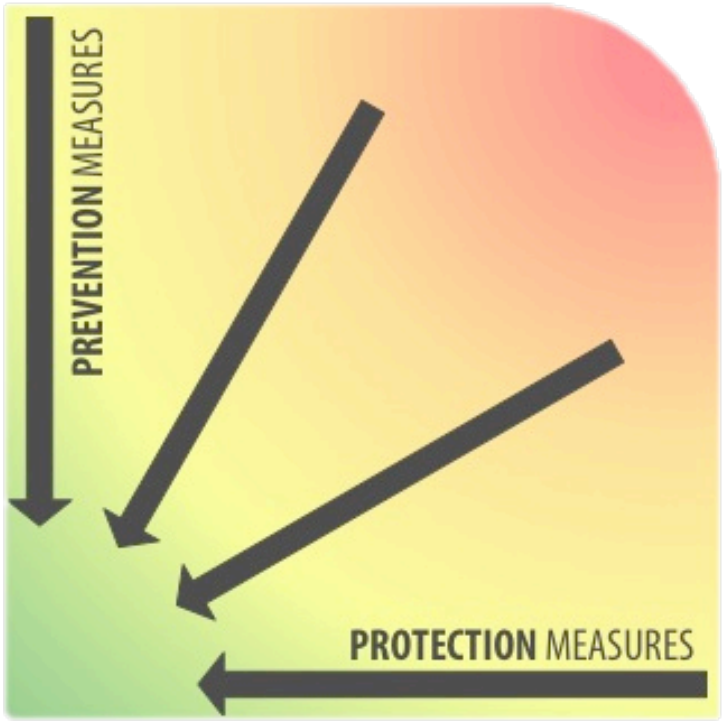
Risk evaluation Matrix (the simplest one)

		Likelihood of occurence		
		LOW	MEDIUM	HIGH
Consequence	LOW	**LOW RISK**	**LOW RISK**	**MEDIUM RISK**
	MEDIUM	**LOW RISK**	**MEDIUM RISK**	**HIGH RISK**
	HIGH	**MEDIUM RISK**	**HIGH RISK**	**HIGH RISK**

Preliminary safety reports Demonstrative part (2/2)

- Risk responses/treatments
  - **Technical** (**structural**) measures or provisions implemented to mitigate the risks
    Conception documents (notes, drawings…)
    Zoning principles
    Calculation notes…
  - **Organizational** measures or provisions planned to mitigate the risks
    Outline of the instructions and procedures
  - **Operations thresholds**

Risk treatment Protection vs. Prevention

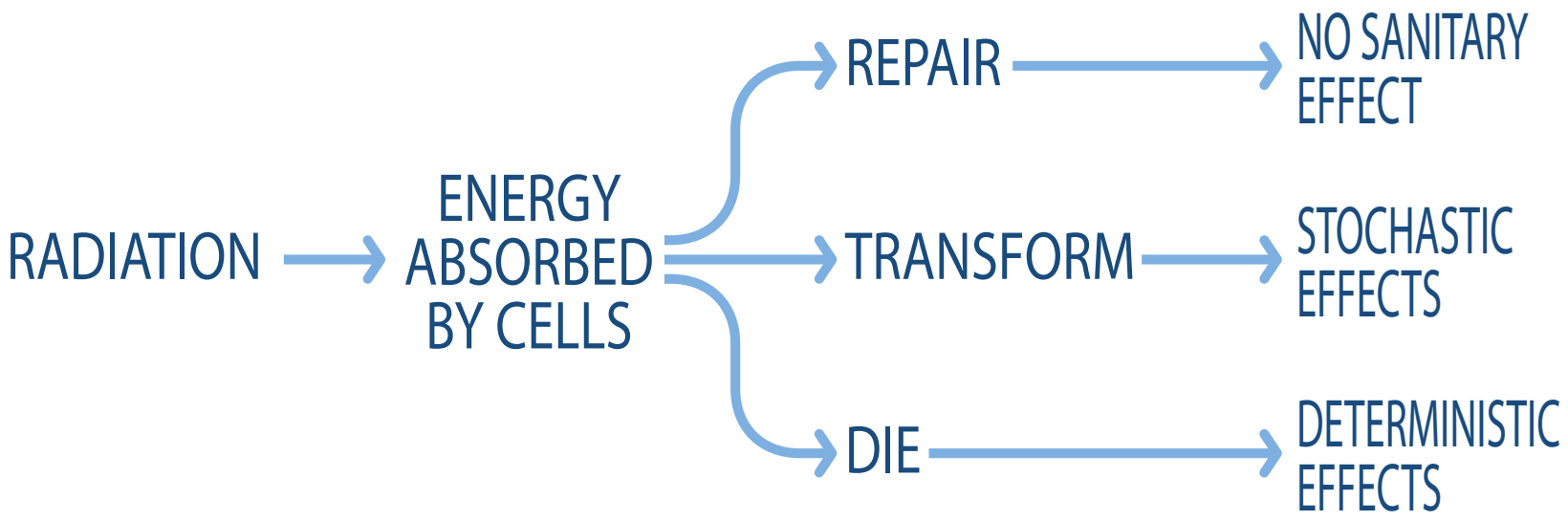


Risk treatment f(risk level)

Preliminary safety reports Safety philosophy

All (most) nuclear safety regulations suggests that individual exposures and number of exposed persons is maintained to a level that is **a**s **l**ow **a**s **r**easonably **a**chievable, (i.e. **ALARA**) taking into account economical and social factors.

Preliminary safety reports Safety philosophy



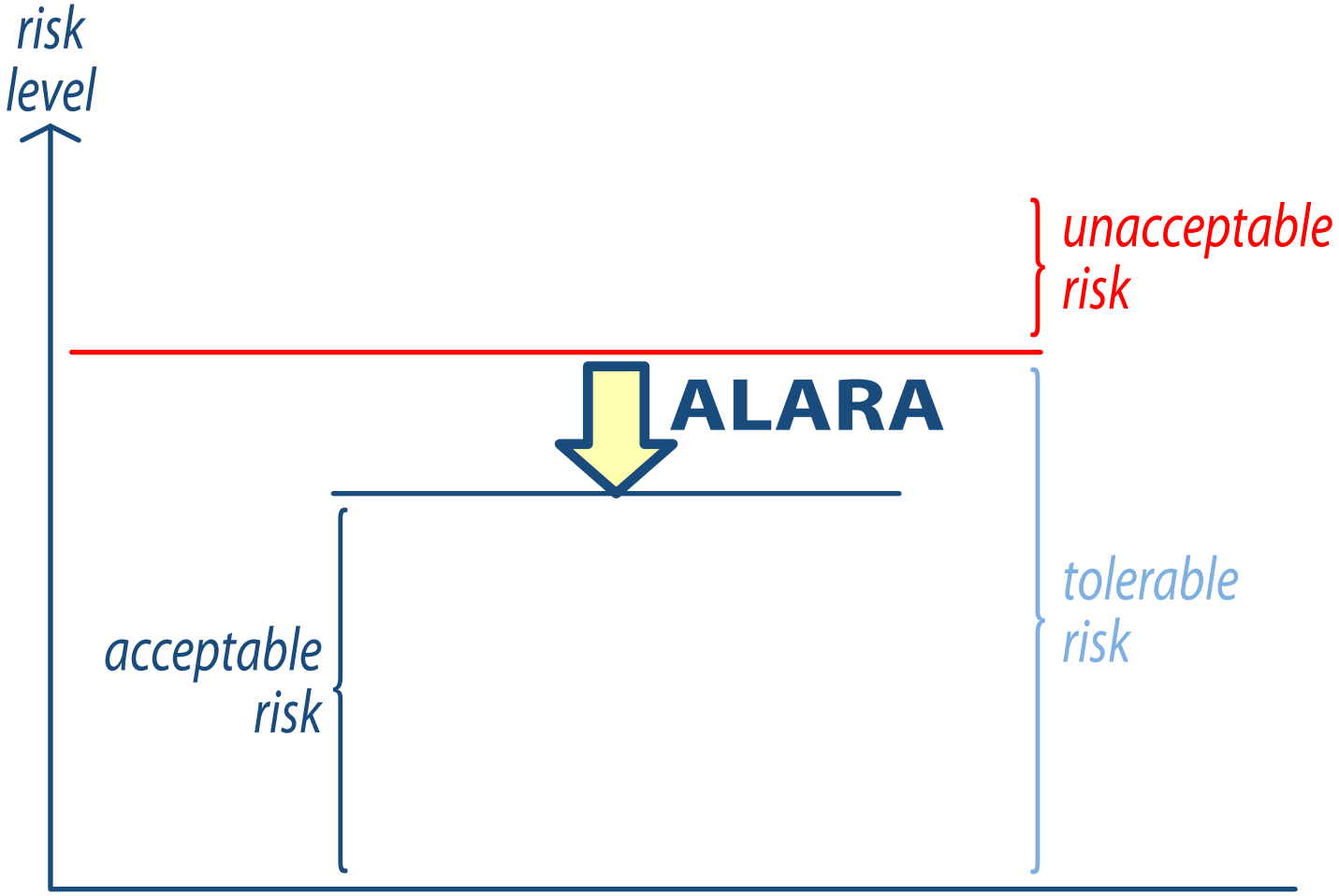
DETERMINISTIC EFFECTS

- Effect = f(dose)
- Gravity = f(dose)
- Early effects
- ∃ thresholds
- Probability = 1

STOCHASTIC EFFECTS

- Effect ≠ f(dose)
- Gravity ≠ f(dose)
- Late effects
- **“No threshold”**
- Probability = f(dose)

Preliminary safety reports Safety philosophy



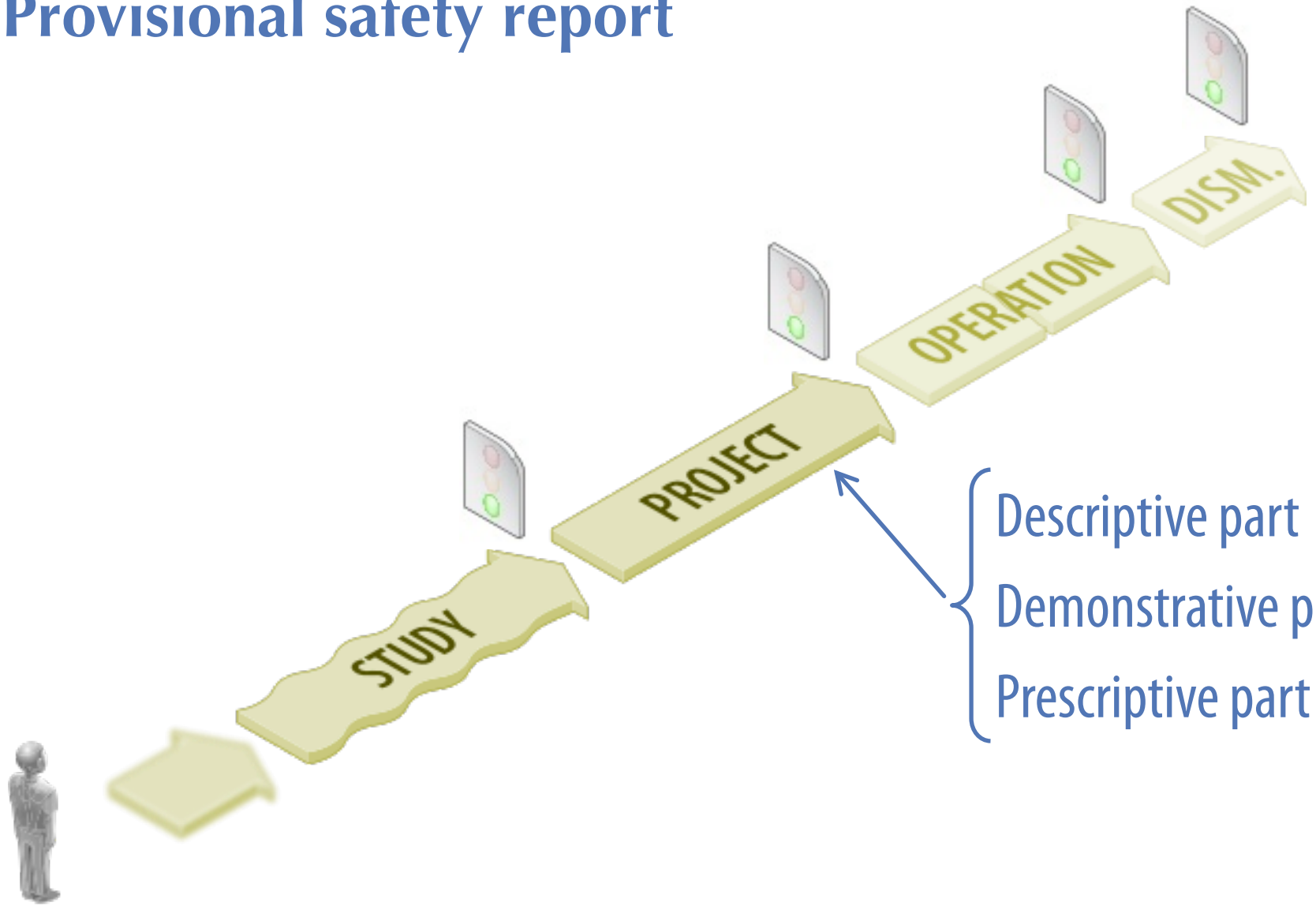
Preliminary safety reports Safety philosophy

Practically:

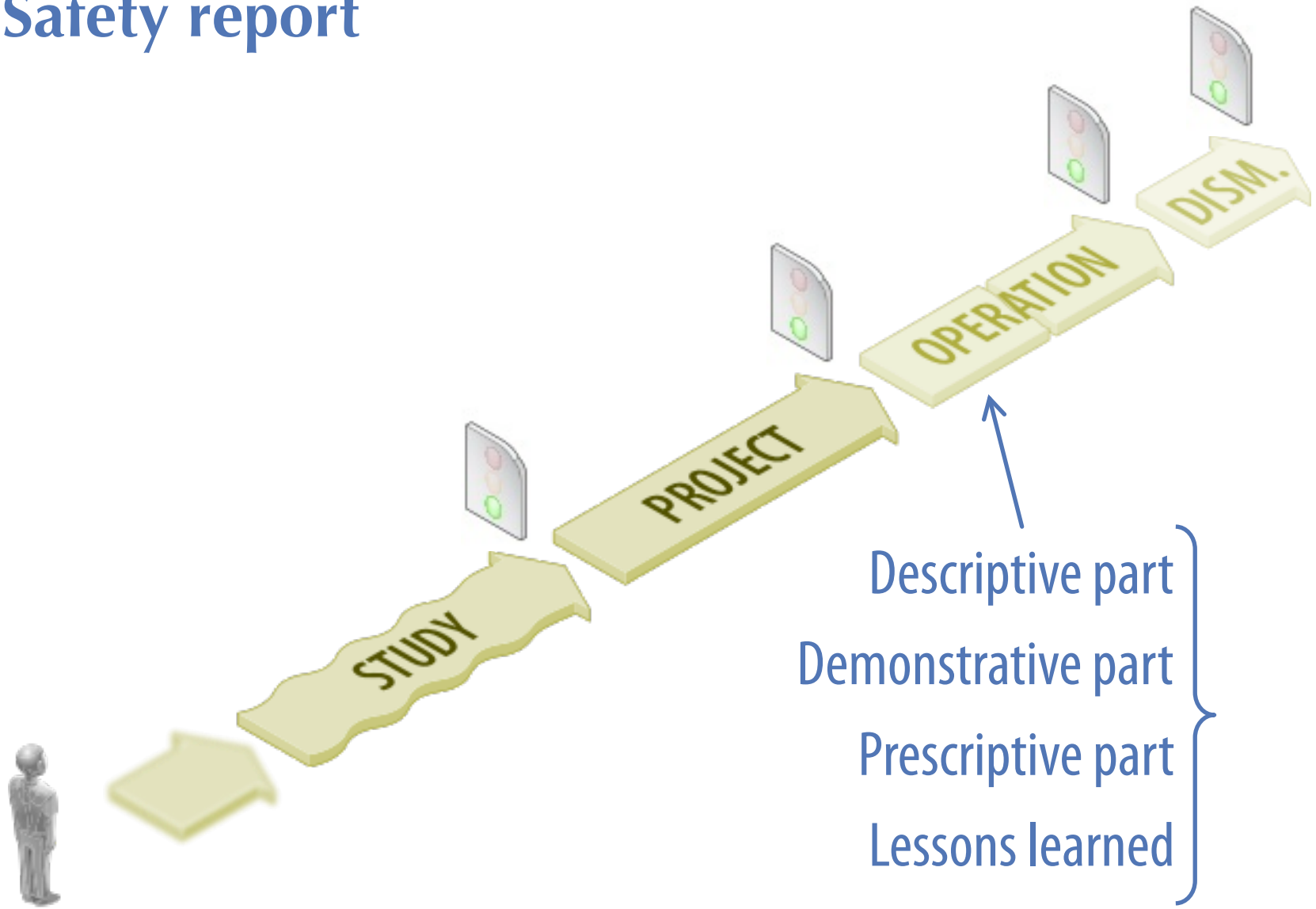
For a given hazardous situation,

- Evaluate risk level (radiation exposure…)
- Identify possible protection and prevention, structural and organizational treatments
- Estimate their impact on the performance (incl. construction/operation costs and schedule)
- Select the most appropriate one(s)

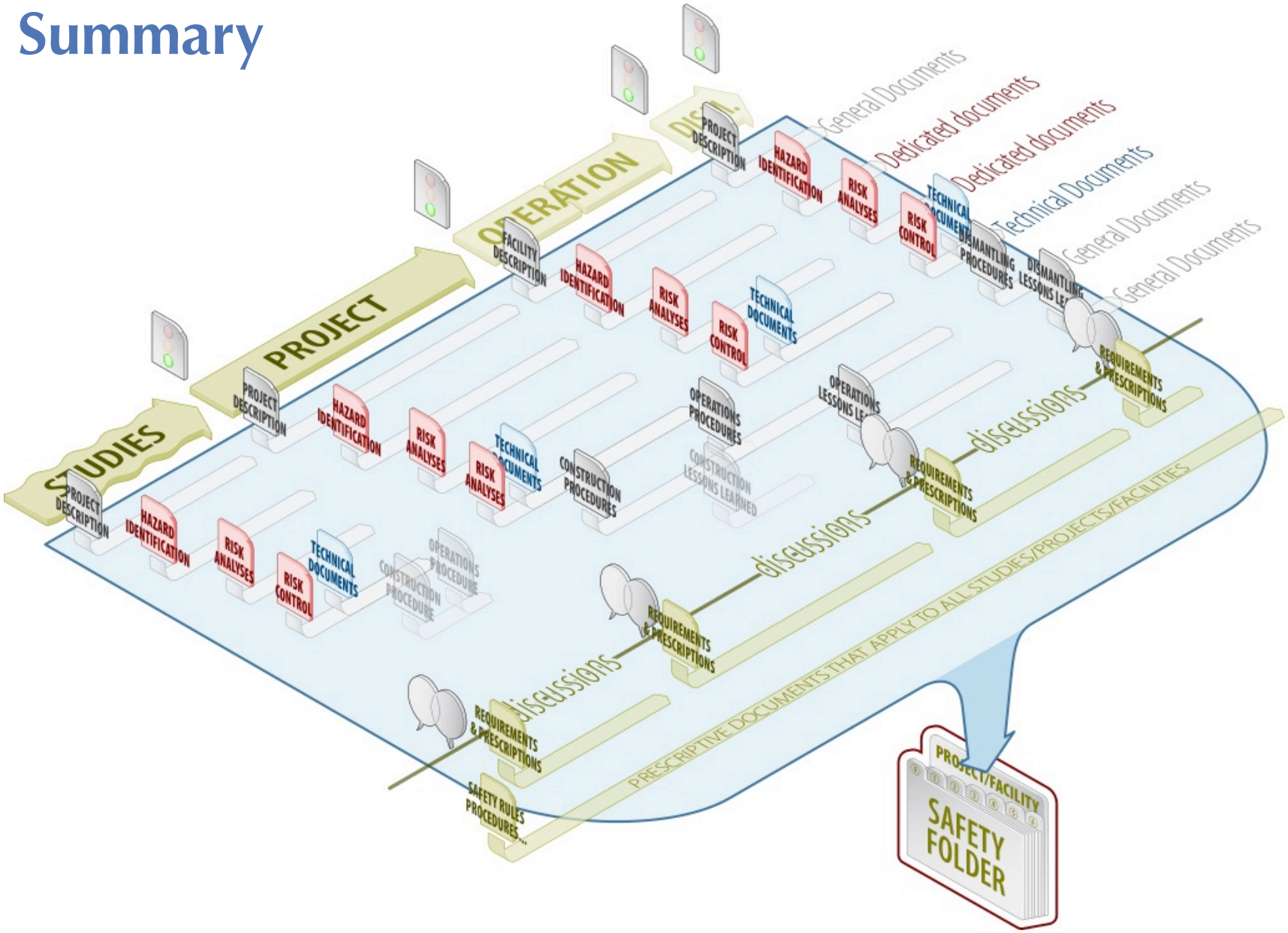
Provisional safety report



Safety report



Summary


STUDIES
PROJECT
OPERATION
PROJECT DESCRIPTION
FACILITY DESCRIPTION
HAZARD IDENTIFICATION
RISK ANALYSES
RISK CONTROL
TECHNICAL DOCUMENTS
CONSTRUCTION PROCEDURES
OPERATIONS PROCEDURES
CONSTRUCTION LESSONS LEARNED
OPERATIONS LESSONS LEARNED
DISMANTLING PROCEDURES
DISMANTLING LESSONS LEARNED
General Documents
Dedicated documents
Dedicated documents
Technical Documents
General Documents
General Documents
discussions
discussions
discussions
REQUIREMENTS & PRESCRIPTIONS
REQUIREMENTS & PRESCRIPTIONS
REQUIREMENTS & PRESCRIPTIONS
SAFETY RULES PROCEDURES...
PRESCRIPTIVE DOCUMENTS THAT APPLY TO ALL STUDIES/PROJECTS/FACILITIES
PROJECT/FACILITY
SAFETY FOLDER

Who does what?

Editorial work of the safety reports:

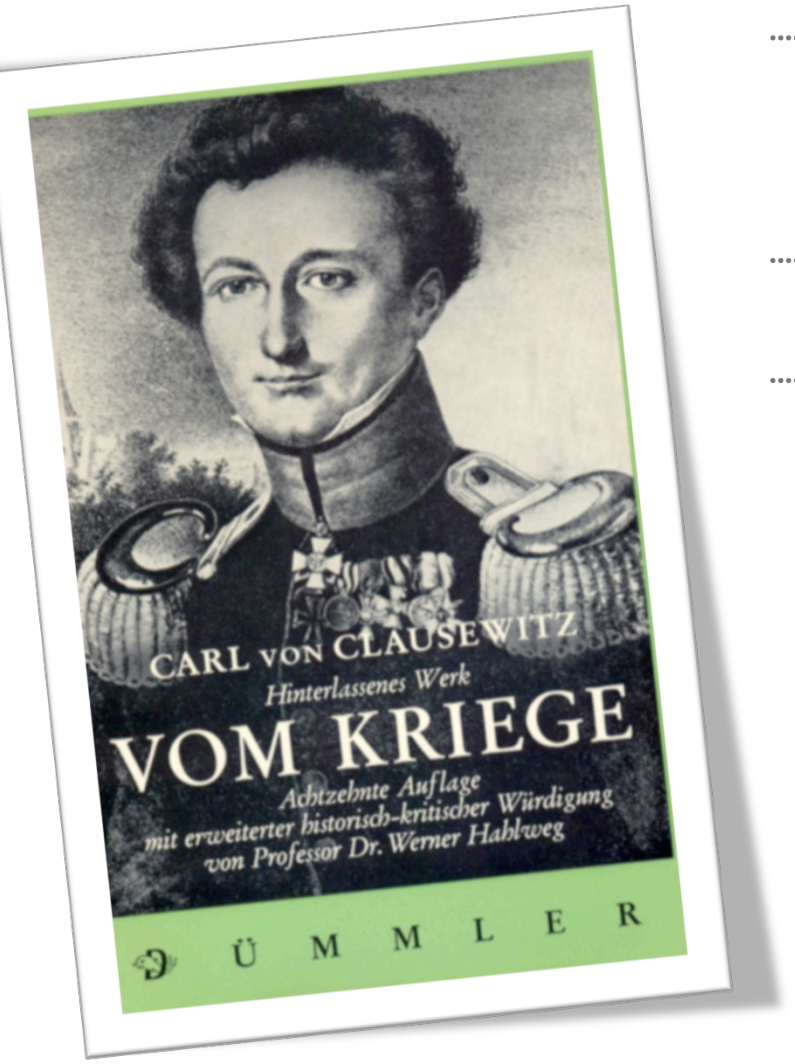
- the duty of the **study/project team**
  (then the duty of the operations team)
- some **safety/integrity engineering skills**
  shall be embedded in the study/project team
- some analysis can be outsourced,
  but the overall responsibility remains
  in the study/project team

Who does what?

If safety/integrity is **correctly embedded** into the conception work, it should not be too painful

If safety/integrity is **kept aside** from conception work, then it may really become a critical issue

Carl von Clausewitz *On War* 19th century



- Focused forces (avoid dissemination)
- Minimize means
- Maximize freedom of action (flexibility)

Thank you

Questions?