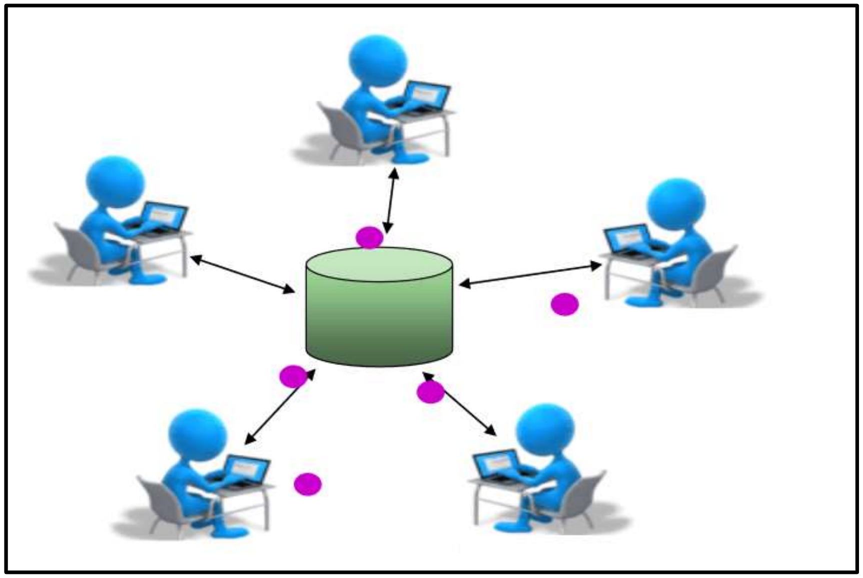
Systems Engineering and Aerospace Design (AE3211-I)

Risk Management, Concurrent Engineering

Prof. Dr. Eberhard Gill



© ESA CDF

Today you'll learn to …

1. **Assess, present and manage risk** in a Systems Engineering framework

2. Understand **need** and **basic elements of Concurrent Engineering**

Both elements are crucial for the upcoming
Design Synthesis Exercise!

© Delft University of Technology

Contents

- Risk Management
  - What is risk?
  - Assessment of risk
  - Handling of risk
  - Tips for the DSE
  - **Exercise**

- Concurrent Engineering (CE)
  - Definition and needs for CE
  - Basic concepts

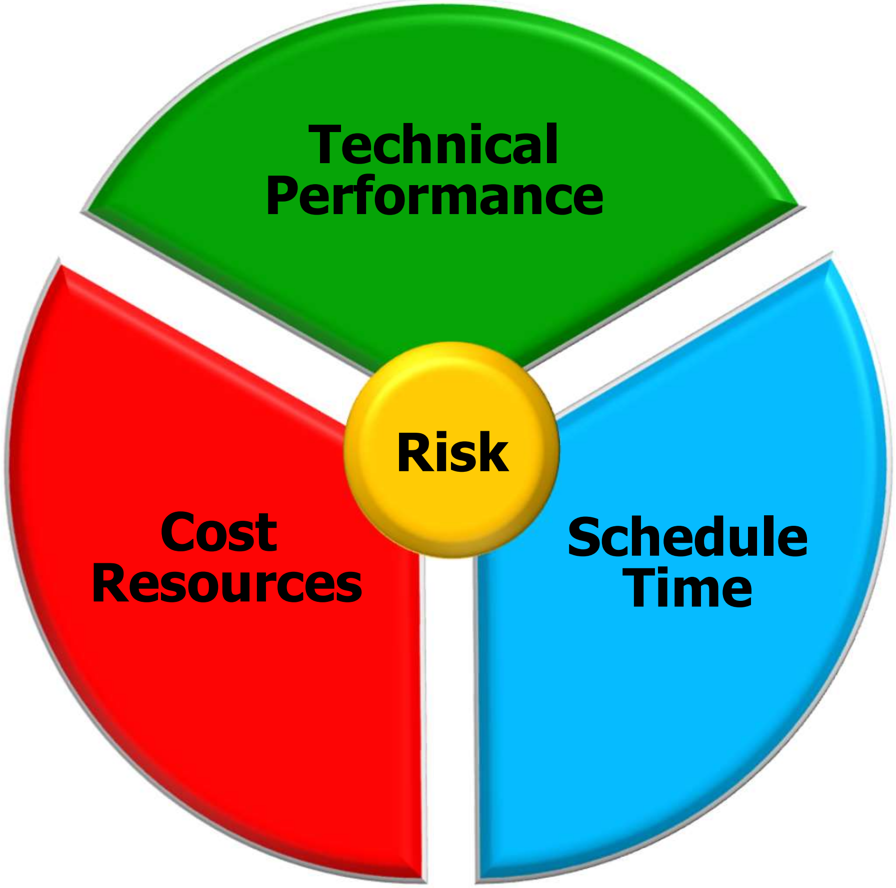
- Summary

Acknowledgement:

The part on risk management was supported by material from Prof. R. Curran and W. Verhagen.

The part on CE was supported by material from ESA/ESTEC and B. Zandbergen.

ReCap: Risk in the Systems Engineering Universe



The Systems Engineering universe is established by technical performance, cost and schedule. All three dimensions are interconnected via **risk**.

What is Risk and its basic Aspects?

- Risk in Systems Engineering

  Measure of **uncertainty of attaining a goal**, objective, or requirement pertaining to technical performance, cost, and schedule

- Risk is **always present**, e.g.
  - Performance near the limits of the state-of-the-art? ⇒ technical risk
  - Purchase item availabile? ⇒ schedule risk
  - Funding constraints limited? ⇒ cost risk

- Interdependency

  technical risk ⇔ schedule risk ⇔ cost risk

- Risk cannot be removed completely, but can be made acceptable.

  ~~Set very low technical goals, stretch schedule and provide unlimited funds.~~ (That's not how the world works!)

Risks are **dynamic**. They change, appear and disappear along your project. Interdependency makes risk **manageable** => trade risks.

Risk Management (in Industrial SE)

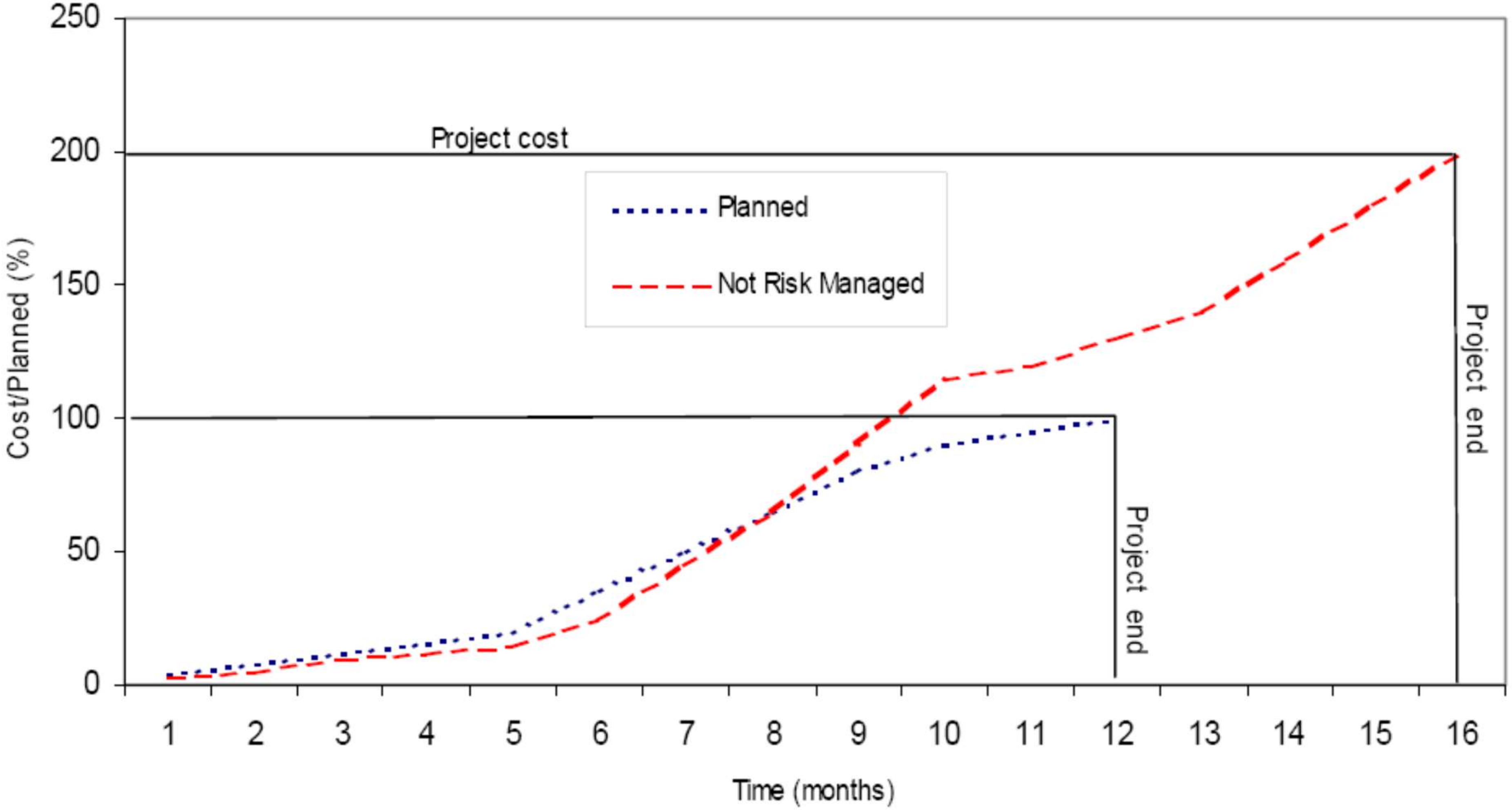
Recognition, assessment, and control of uncertainties that may result in schedule delays, cost overruns, performance problems, adverse environmental impacts, or other undesired consequences

- Recognition: Failure Mode, Effects and Criticality Analysis (FMECA), Fault Tree Analysis (FTA)
- Assessment: qualitative (risk map), quantitative (reliability, FMECA, FTA)
- Control: risk item tracking, budgets, Technical Performance Measurement (TPM). TPM is defined as “the continuing prediction and demonstration of the degree of anticipated or actual achievement of selected technical objectives."

In addition to Project Risk Management (PRM, this lecture), there is Environmental Risk Management (ERM) for environmental, health, safety risks.

SE: Systems Engineering

Impact of Risk Management



Proper Risk Management is KEY to good Systems Engineering.

Example of bad Risk Management: Berlin Brandenburg Airport

Schedule

- Construction started in 2006
- Planned opening in Oct. 2011
- Actually opened in Oct. 2020

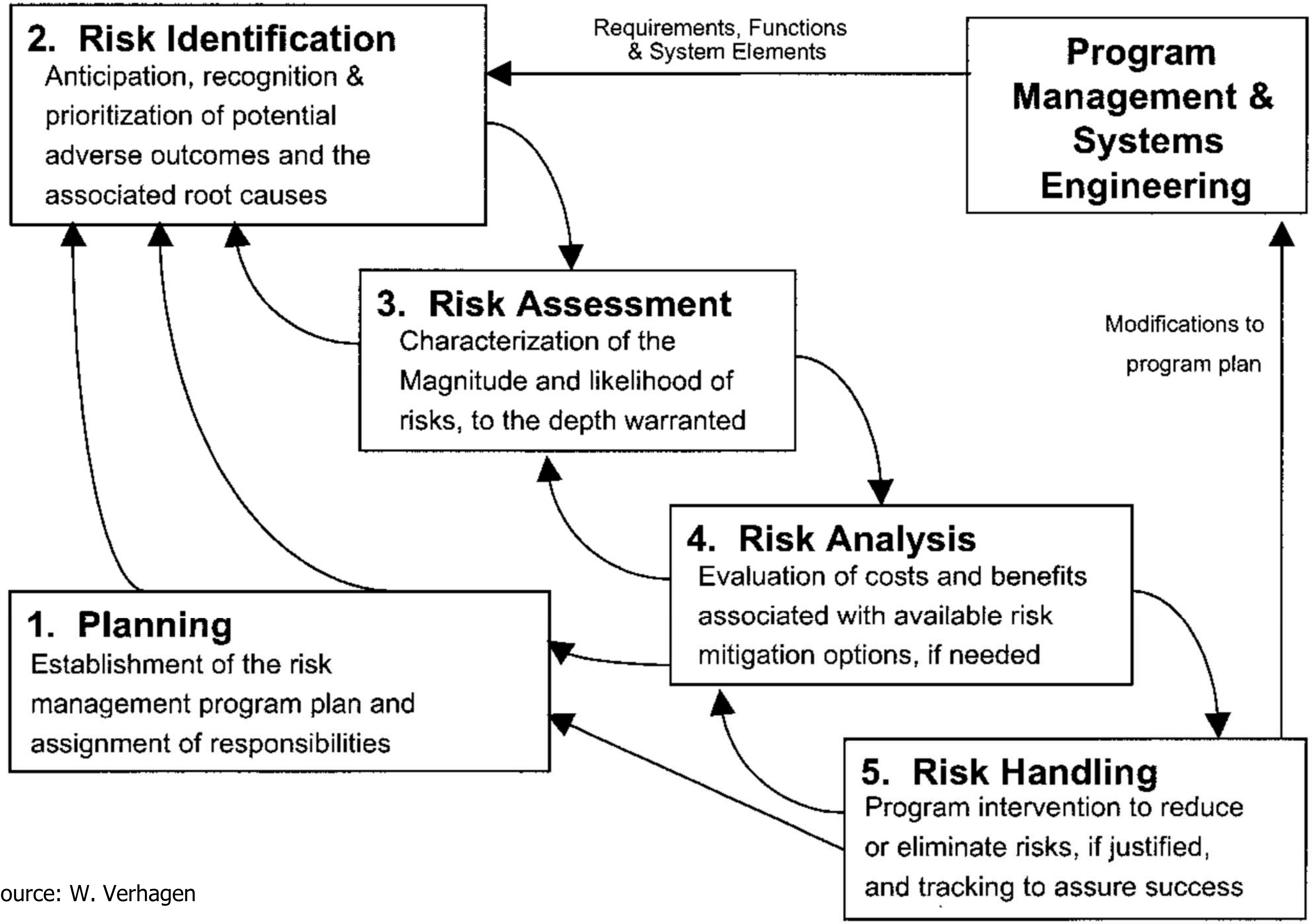
Cost

- Original plan 2 € billion
- Realized cost 7 € billion

Source. Wikipedia

Part of this disastrous development was improper Risk Management.

Risk Management Process



2. Risk Identification
Anticipation, recognition & prioritization of potential adverse outcomes and the associated root causes

Requirements, Functions & System Elements

Program Management & Systems Engineering

3. Risk Assessment
Characterization of the Magnitude and likelihood of risks, to the depth warranted

Modifications to program plan

4. Risk Analysis
Evaluation of costs and benefits associated with available risk mitigation options, if needed

1. Planning
Establishment of the risk management program plan and assignment of responsibilities

5. Risk Handling
Program intervention to reduce or eliminate risks, if justified, and tracking to assure success

Source: W. Verhagen

Technical Risk Assessment

Techniques for technical risk assessment during a development project (to be done **continuously** and **in each step** of project development):

- **Identification** of (potential) risks
- Assessment of "**probability**" of occurrence
- Assessment of "**seriousness of impact**" on performance, schedule & cost
- **Ranking** of risks
- Indicating preferred **measures** for risk handling

Objective is to spend scarce resources (people, money, time) in those areas where they will achieve the largest necessary reduction in risk.

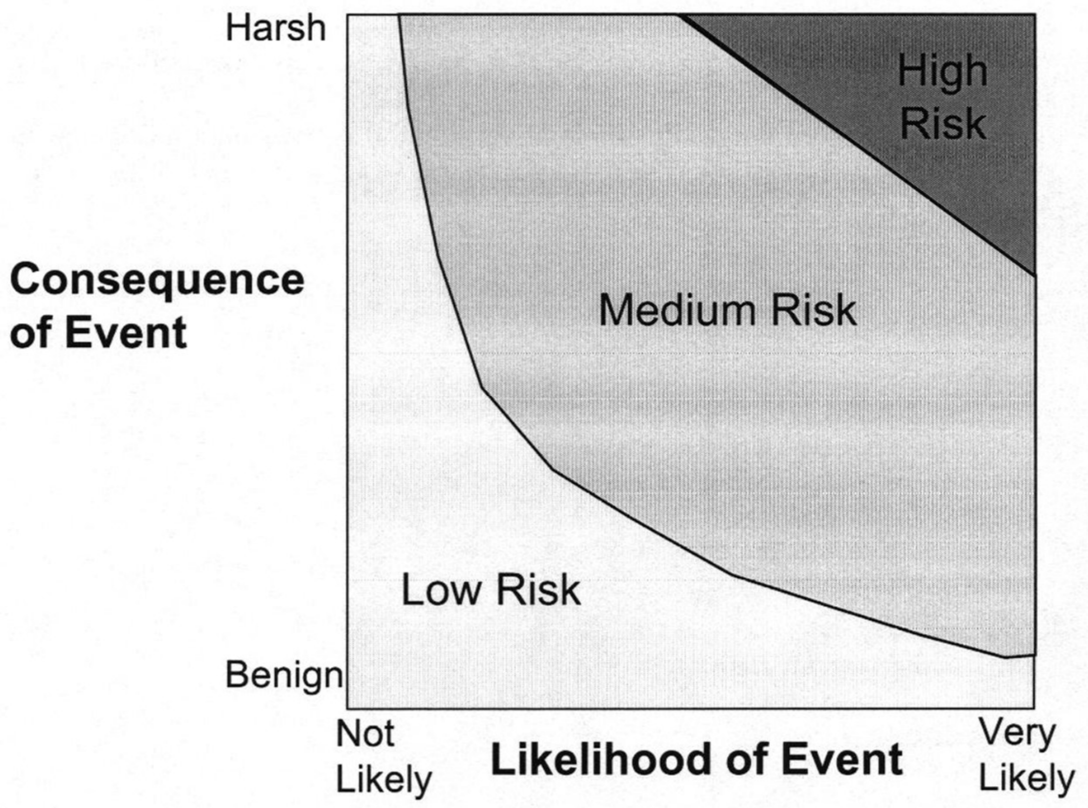
To be most effective, risk assessment shall be an integral part of the (technical) project work.

Risk Map, a Systems Engineering Tool

Risk = **Likelihood** of event * **Consequence** of event

Required Methods:

1. Identify events
2. Evaluate likelihood of event (qualitative or quantitative)
3. Evaluate consequence of event



Note: X- and Y-axis are sometimes interchanged.

Metrics of Risk Map (Examples)

Severity of consequence: e.g. be expressed as a consequence for the mission or mission criticality

- **Catastrophic**: mission failure or significant non-achievement of performance
- **Critical**: mission success is questionable or some reduction in technical performance
- **Marginal**: Degradation of secondary mission or small reduction in technical performance
- **Negligible**: inconvenience or non-operational impact

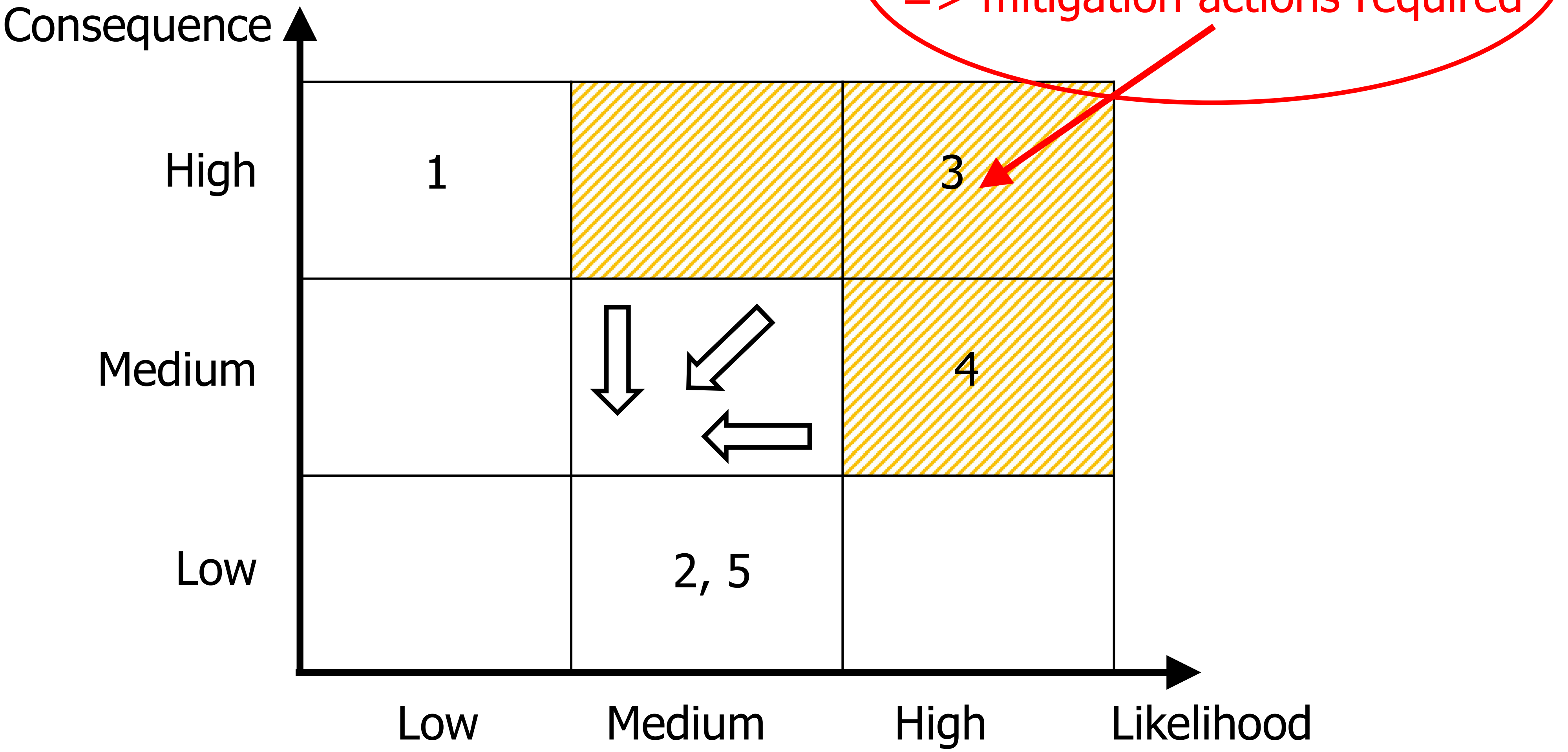
in order of decreasing severity of impact

Probability (PR) of occurrence: e.g. function of state or maturity of technology (values are samples)

- Very high (5); PR >= 70%
- High (4); 50% <= PR < 70%
- Moderate (3); 30%<=PR<50%
- Low (2); 1% <= PR < 30%
- Very low (1); PR < 1%

Number of categories for consequence and likelihood in a risk map shall be 3-6. Selected metrics types depend on Risk Management approach.

Risk Mitigation



Zone of non-tolerated risks
=> mitigation actions required

Project Managers and System Engineers should not manage more than 6-10 risks each, so must other key team members!
Risk registers with hundreds of risks can be “counter-productive”.

Numbers in the risk map are individual risks. You will have a numbered list of risks, to link risk and their associated numbers.

Risk Mitigation Strategies

Risk mitigation = getting rid of unacceptable risks, i.e. the technical approach to risk reduction

Four different strategies for defining action plans:

1. **Remove** the risk (e.g. change your design)
2. **Reduce** the risk (e.g. by decreasing its likelihood (prevent) of occurrence and/or its consequence (mitigate) or a combination)
3. **Accept** the risk, while monitoring it (e.g. via power budget)
4. **Transfer** or share the responsibility to/with a third party to globally optimize technical performance, schedule and cost (e.g. insurance or other options)

In reality, it is often a combination of the four strategies.

Technical Resource Management

Technical resource **budgets**:

Subset of the set of technical parameters that determines the success or failure of a development project

- Typically **scarce or expensive resources** (e.g. mass, power and computer capacity of aerospace vehicles)
- **Margin** between required value and actually achieved value of these resources (shall decrease continuously during the execution of a project)

Risk Management is to a large extent Technical Resource Management.

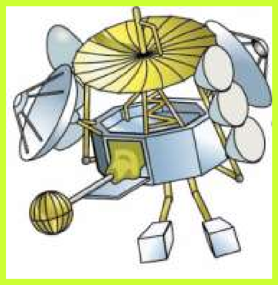
Sample Technical Budgets

Aircraft

- Weight
- Aircraft availability
- Drag
- Center of gravity location
- Thrust
- Take-off/ landing maximum lift
- Series production cost
- Cruise specific fuel consumption
- Direct maintenance cost
- …

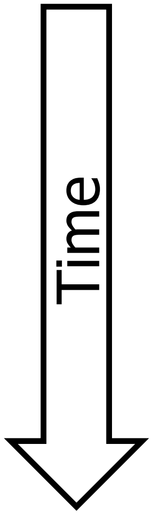
Spacecraft

- Mass
- On-board computer capacity
- Electrical power
- Pointing error
- Delta V
- Propellant mass
- Communication link
- Volume
- (Series) production cost
- …



Evolution of Contingency Margin

Allowance of contingency (%) in computer resources

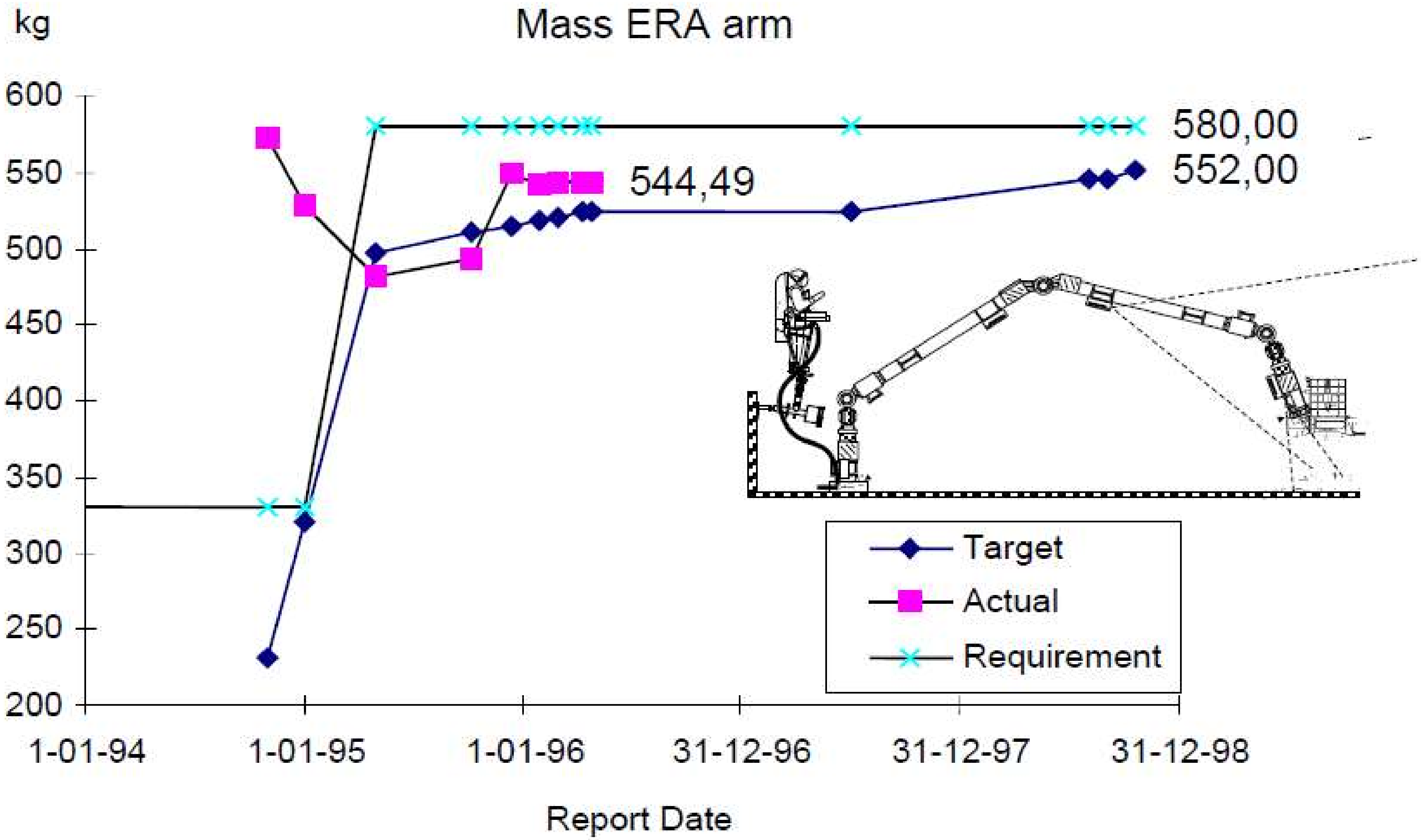


Design Maturity	Mass Memory size	ROM size	RAM size	CPU load
URD	40	40	40	60
SRD and ADD	35	30	30	50
DDD and Coding	30	25	25	25
HW-SW Integration	-	20	15	20
QM software	25	15	10	15
FM software	20	10	5	10

Note: Values selected for a project which allows in-flight software upgrade. Values are margins of computer resources, not computer resources itself.

URD User Requirements Document
SRD Software Requirements Document
ADD Architectural Design Document
DDD Design Description Document
QM Qualification Model
FM Flight Model
ROM Read-Only Memory
RAM Random Access Memory
HW-SW Hardware-Software

European Robotic Arm (ERA) Mass Budget



Budget Control Mechanisms

Actions need to be taken if:

- the actual value exceeds the target (comparison excluding contingencies)
- the actual value exceeds the specification (comparison including contingencies); includes design maturity aspects

Options on actions:

1. Decrease uncertainty in design (bread-boarding, tests, design review)
2. Change the specification value
3. Modify the design

A budget can be established for many different technical aspects.

DSE: Applying Risk Management

Produce a **Risk Map** and a **Risk Mitigation Plan** (what you are going to do to bring the risk back to acceptable proportions) for your design

1. Determine the list of elements/functions to include in the risk map
2. Define the steps you will use in the assessment of the probability of occurrence of "things going wrong"
3. Define the steps you will use in the assessment of the consequence when the risk occurs
4. Plot the elements in a Risk Map with the highest risks in the top-right corner

DSE: Applying Risk Management (cont’d)

Produce a **Risk Map** and a **Risk Mitigation Plan** (what you are going to do to bring the risk back to acceptable proportions) for your design

5. Define for each high risk element the mitigation measures you will take

6. Generate a ‘posterior’ Risk Map which shows the anticipated effect of mitigation

7. Risk item tracking: check the status of risks and mitigation on regular basis

Lessons from DSE Experience

- Use **meaningful scales**: numbers may sound reliable, but quantification is usually not available in conceptual design!

- Put priority on identification of **technical risks** while designing, even in conceptual design:

  "The Fellowship burns down" versus "Li-ion battery thermal run-away" – which do you prefer?

- To iterate: "To be most effective, risk assessment shall be an **integral** part of the (technical) project work."

- Don't forget about mitigation!

Use Risk Management as an **aid**; not see it as formal deliverable only.

Exercise *Risk Management*

Consider the following Project Objective Statement for an example DSE project:

Design a competitively priced, fully recyclable 'green-fuel' Unmanned Aerial Vehicle (UAV) that can autonomously monitor extended forest areas for fire outbreaks, by 10 students in 10 weeks time.

1. Identify at least 5 risks for this UAV and qualitatively estimate the likelihood and impact of occurrence.

2. Plot the associated risk map for the UAV and address the top 2 risks by explaining which risk mitigation measures you will take.

What is Concurrent Engineering?

Concurrent Engineering (CE) is a systematic approach to ***integrated product development*** *that emphasizes the response to customer expectations.*

It embodies team values of co-operation, trust and sharing in such a manner that decision making is by consensus, involving all perspectives in parallel, from the beginning of the product life cycle. (Definition: ESA)

The ESA/ESTEC **Concurrent Design Facility (CDF)** is an Integrated Design Environment (IDE) available to all ESA programs for interdisciplinary applications based on the CE methodology.

Key usage: **Conceptual design** of future space missions, i.e. internal pre-phase A and feasibility studies.

Auxiliary usage: Reviews, project lessons, educational activities, …

Traditional Design Process

Sequential Design („Over-the-fence“ approach)

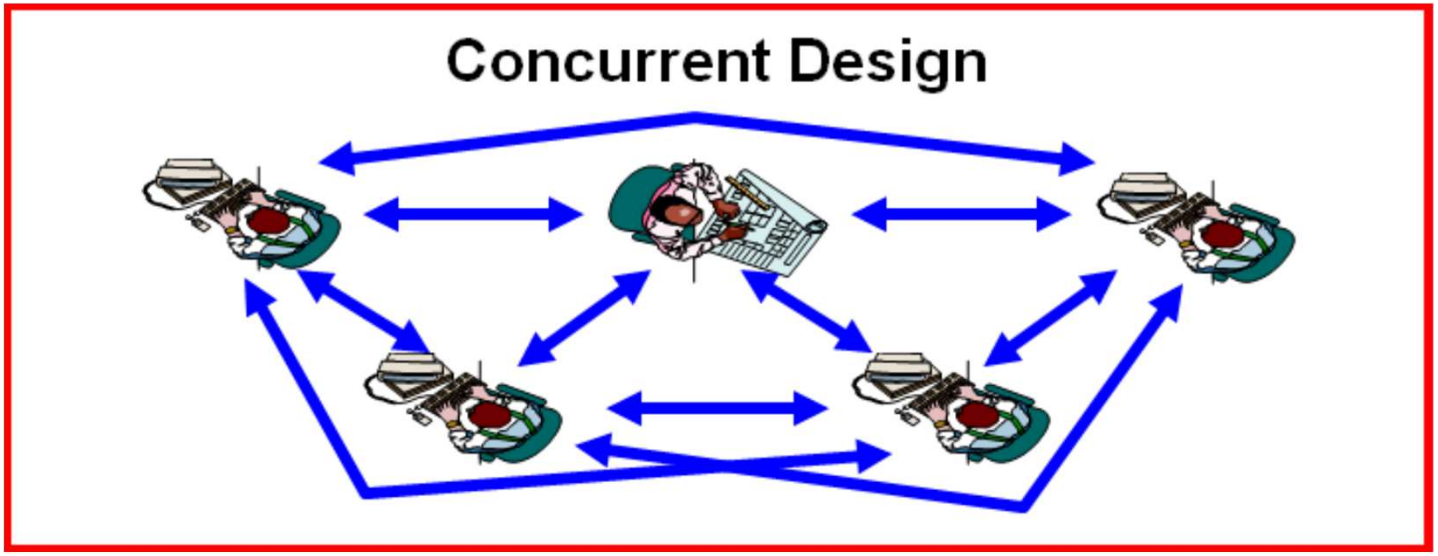
Source. ESA

Sequential Design is, given the fierce commercial competition, neither efficient, nor is it, given the complexity of systems, even effective.

Why Concurrent Engineering?

In the **Design Phase**: to overcome the communications gaps between the „designer" (who produces design information) and the „user" (who utilizes the design information)

In the **Development Phase**: to reduce the risk of development changes in later phases, which imply to halt the development and go back to the „drawing table".



Source. ESA

Benefits Concurrent Engineering @ ESA

Performances (typical pre-Phase A study):

- Study duration (Design phase): 3-6 weeks (before 6-9 months!)
- Factor 4 reduction in time
- Factor 2 reduction in cost (for the Customer)
- Increased # of studies per year; max. 2 parallel studies

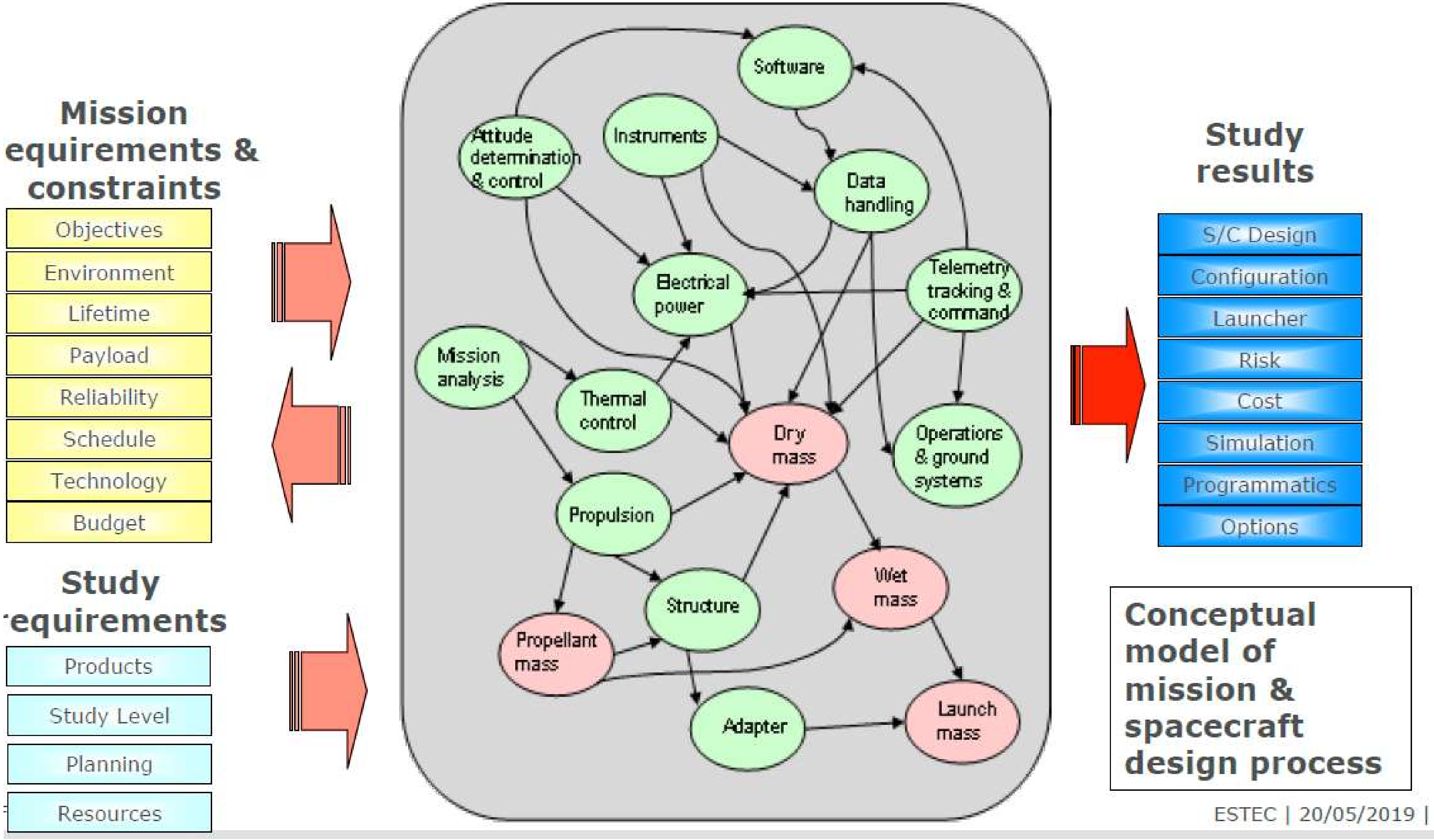
Improvement in quality, providing quick, consistent and complete mission design, incl. technical feasibility, programmatics, risk, cost

Technical report becomes part of the specs for subsequent industrial activity.

Capitalization of corporate knowledge for further reusability

Source. ESA

Design Process



Mission equirements & constraints

- Objectives
- Environment
- Lifetime
- Payload
- Reliability
- Schedule
- Technology
- Budget

Study equirements

- Products
- Study Level
- Planning
- Resources

Study results

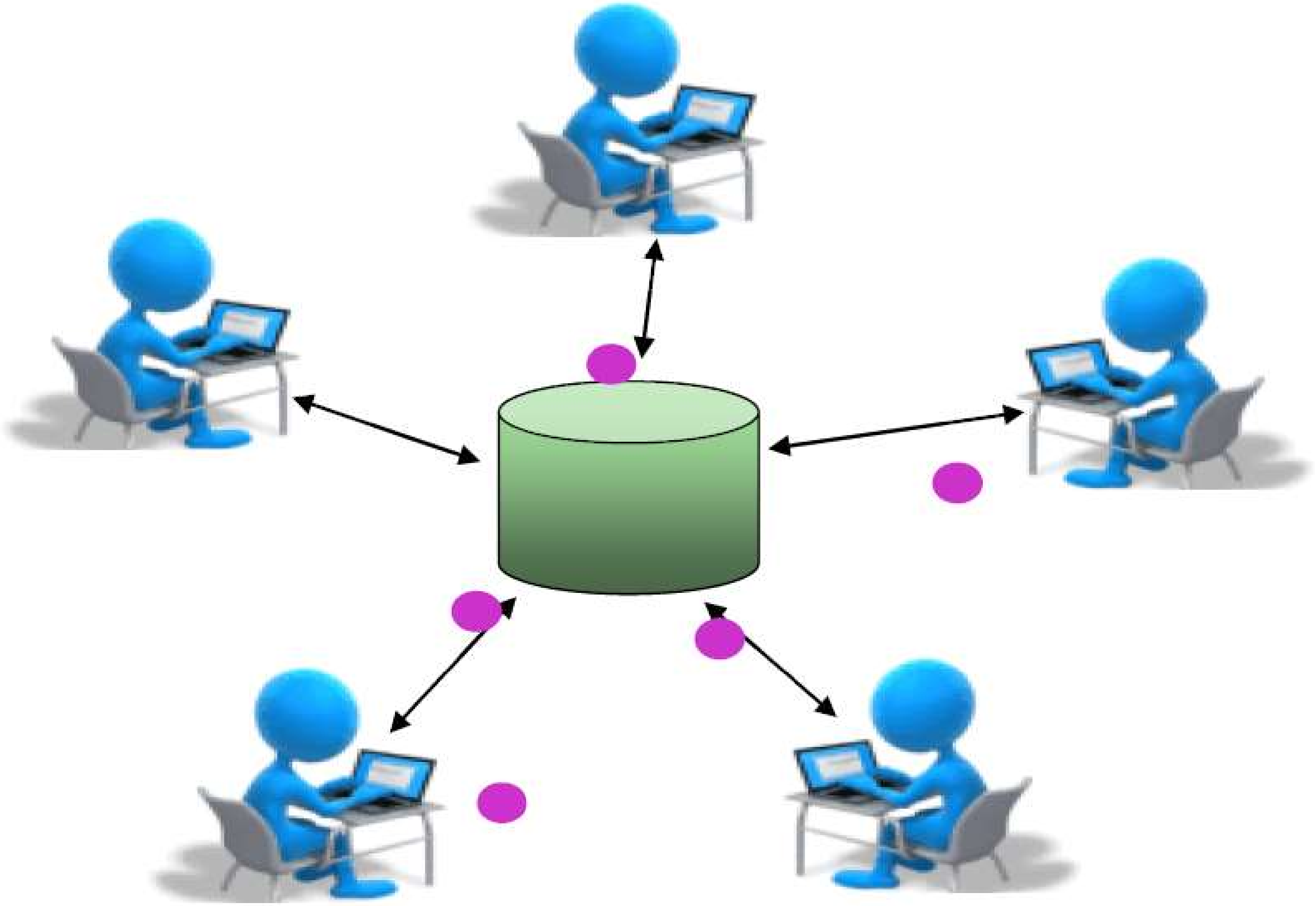
- S/C Design
- Configuration
- Launcher
- Risk
- Cost
- Simulation
- Programmatics
- Options

Conceptual model of mission & spacecraft design process

ESTEC | 20/05/2019 |

Source. ESA

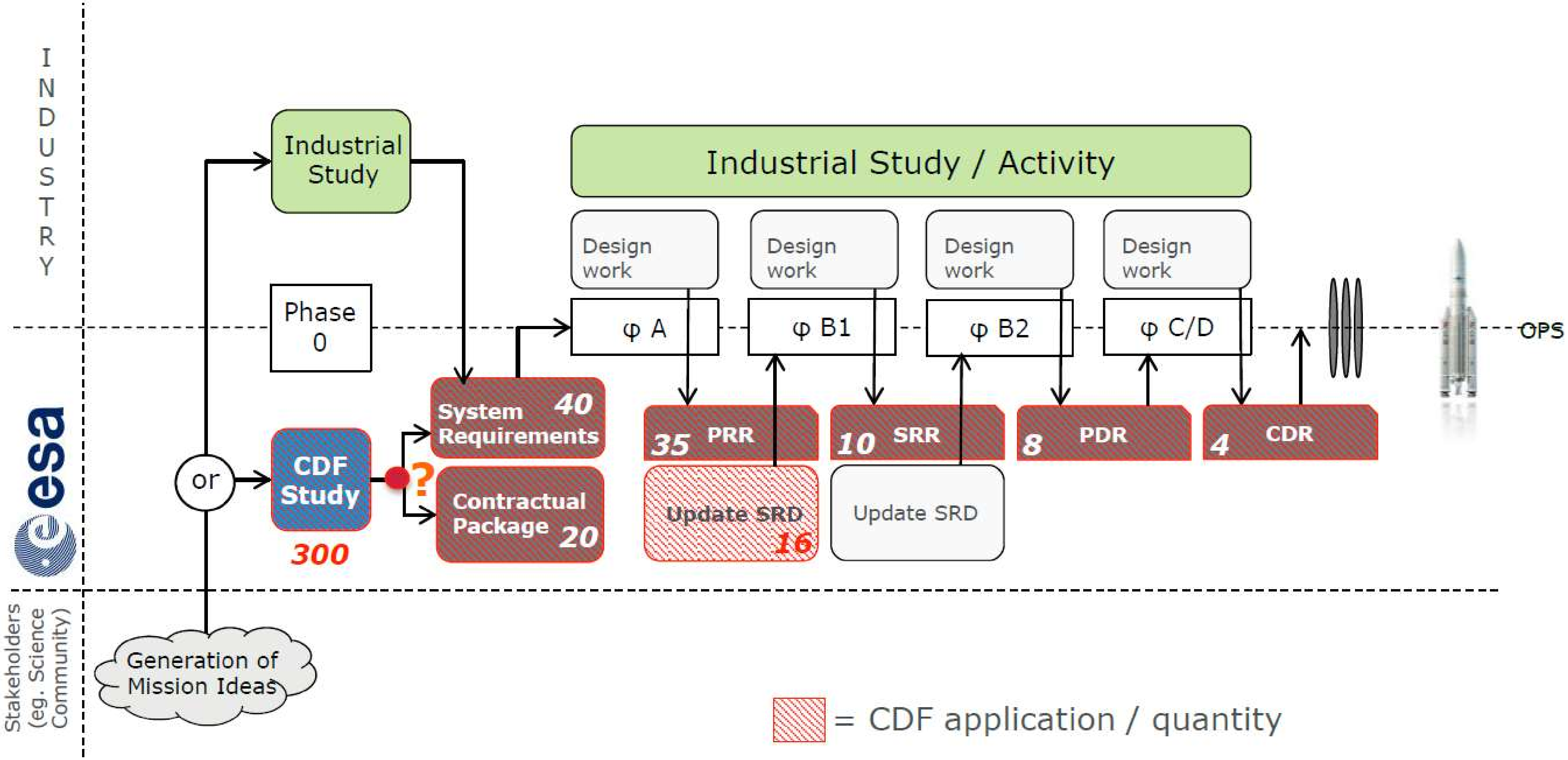
CDF Team & Central Data Repository



Source. ESA

Communication Functions, Central Data Repository and a Open Concurrent Design Tool (OCDT) Software are crucial facilities for a CDF.

Project Lifecycle



Source. ESA

Note: Values are related to CE effort

CDF Concurrent Design Facility
PDR Preliminary Design Review

PRR Preliminary Requirements Review
CDR Critical Design Review

SRR System Requirements Review
SRD System Requirement Document

Online Interdisciplinary Communications

Approach:

- Multidisciplinary
- Holistic
- Systematic
- Centralized
- Focus on Customer expectations
- …

Methodology:

- Iterative presentat.
- Debate
- Consensus
- System awareness
- …

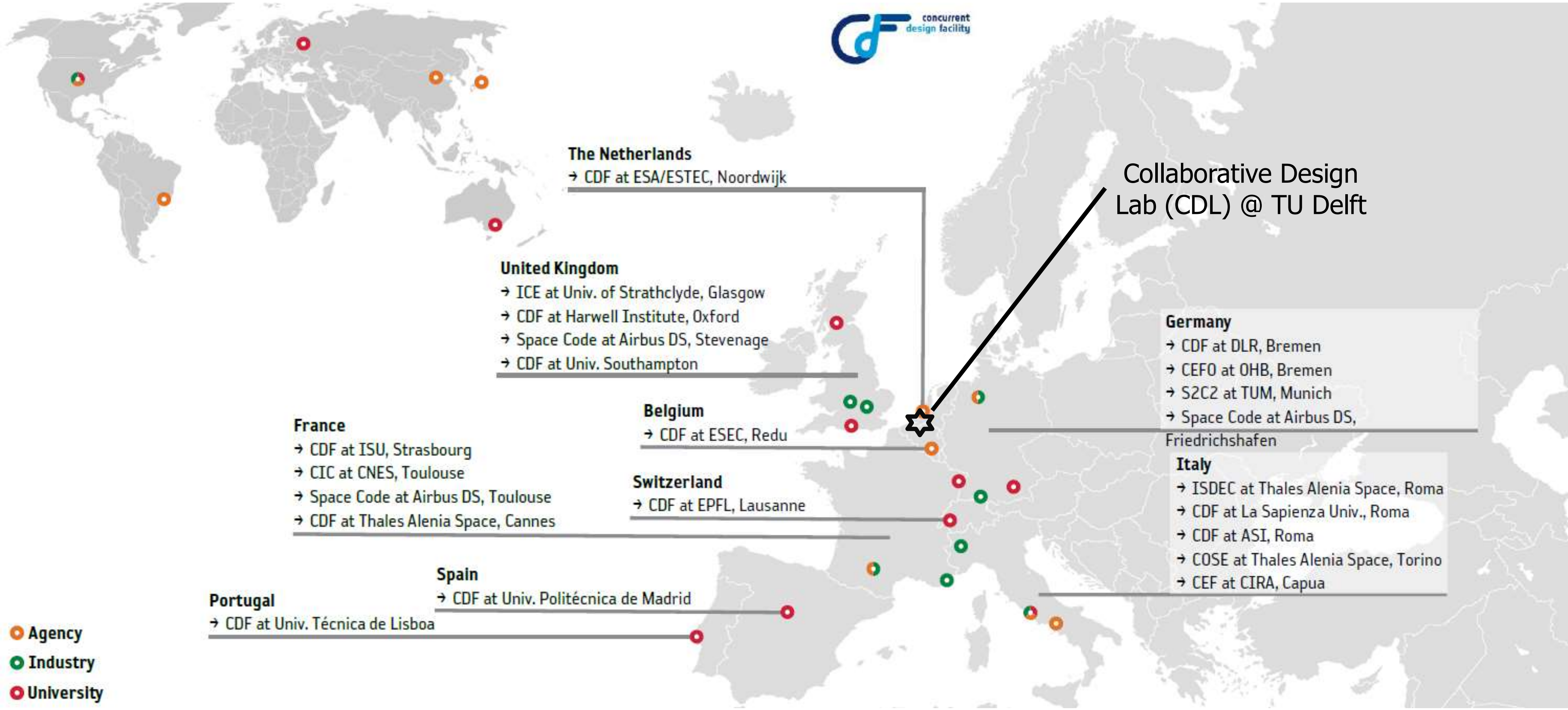
Source. ESA

ESA CDF Mission Studies and Reviews

concurrent design facility
SUN
MERCURY
VENUS
SPACE INFRASTRUCTURE & TECHNOLOGY
LAUNCHERS & RETURN VEHICLES
MOON
EARTH
MARS
ASTEROIDS
JUPITER
SATURN
URANUS
NEPTUNE
PROGRAMMES
GEN. STUDIES
TELECOM
OPERATIONS
EXPLORATION
EDUCATION
EARTH OBS.
LAUNCHER
SCIENCE
NAVIGATION
European Space Agency

Source. ESA

Concurrent Design Centers inspired by ESA



The Netherlands
→ CDF at ESA/ESTEC, Noordwijk

Collaborative Design Lab (CDL) @ TU Delft

United Kingdom
→ ICE at Univ. of Strathclyde, Glasgow
→ CDF at Harwell Institute, Oxford
→ Space Code at Airbus DS, Stevenage
→ CDF at Univ. Southampton

Germany
→ CDF at DLR, Bremen
→ CEFO at OHB, Bremen
→ S2C2 at TUM, Munich
→ Space Code at Airbus DS, Friedrichshafen

France
→ CDF at ISU, Strasbourg
→ CIC at CNES, Toulouse
→ Space Code at Airbus DS, Toulouse
→ CDF at Thales Alenia Space, Cannes

Belgium
→ CDF at ESEC, Redu

Switzerland
→ CDF at EPFL, Lausanne

Italy
→ ISDEC at Thales Alenia Space, Roma
→ CDF at La Sapienza Univ., Roma
→ CDF at ASI, Roma
→ COSE at Thales Alenia Space, Torino
→ CEF at CIRA, Capua

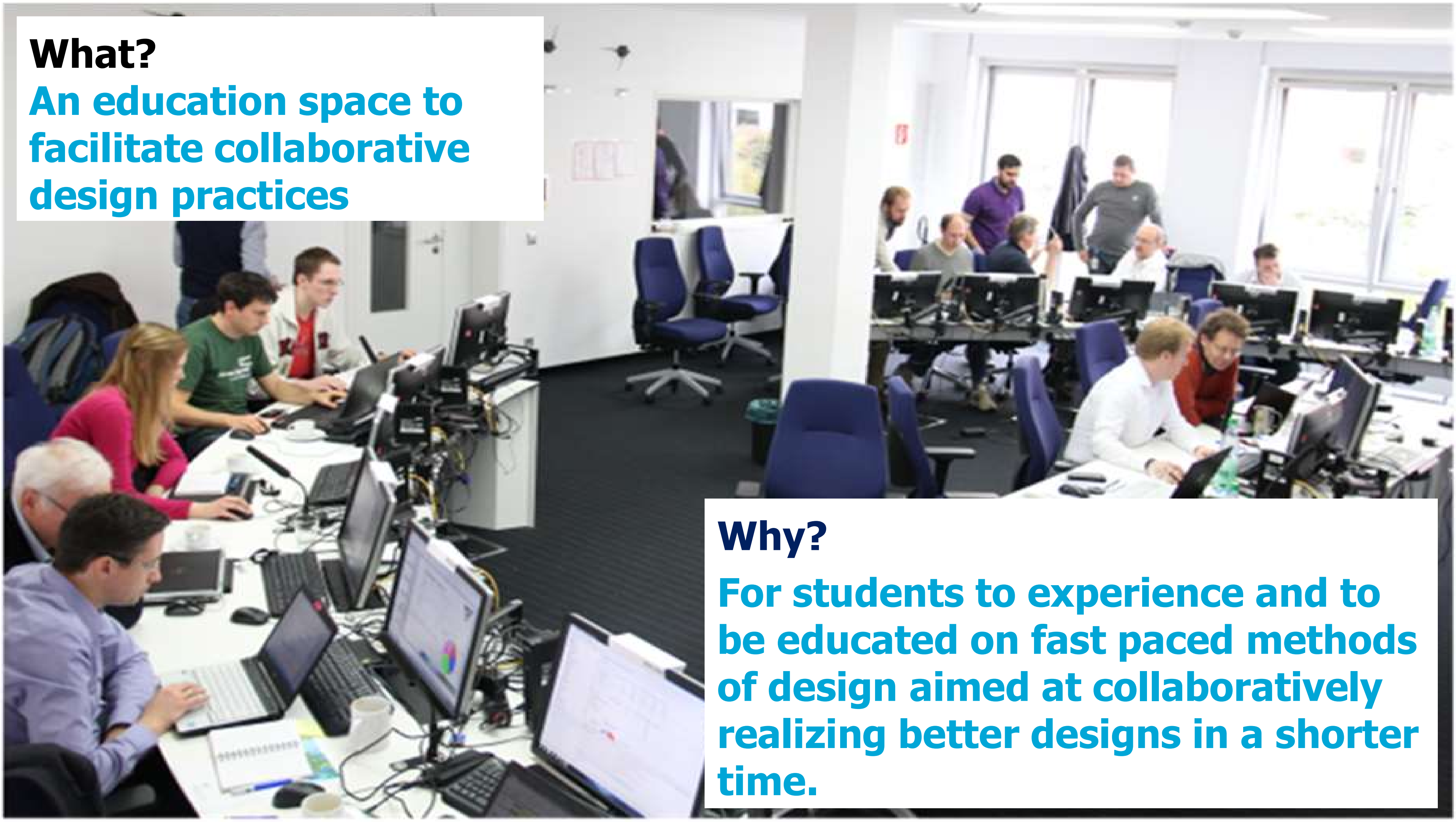
Spain
→ CDF at Univ. Politécnica de Madrid

Portugal
→ CDF at Univ. Técnica de Lisboa

○ **Agency**
○ **Industry**
○ **University**

Source. ESA

Collaborative Design Laboratory (CDL) @ Aerospace Engineering of TU Delft



What?

An education space to facilitate collaborative design practices

Why?

For students to experience and to be educated on fast paced methods of design aimed at collaboratively realizing better designs in a shorter time.

What you have learned

Risk Management

- What is risk
- How to assess and communicate risks
- How to manage risks

Concurrent Engineering (CE)

- The benefits and needs
- Key approaches

Both Risk Management and Concurrent Engineering are important in your upcoming **Design Synthesis Exercise**.

Homework:

- Do the exercises for this lecture (on BrightSpace). Sample solutions are also provided.

Appendix:

- General literature on Systems Engineering, Specific literature on risk management and CE

General Literature

- Wertz J.R., Larson W.J.; Space Mission Analysis and Design; Third Edition; Microcosm, Inc. (1999)

  The classics on Space Mission Analysis and Design with excellent content.

Specific Literature

- ECSS-M-ST-80C – Risk management
- ECSS-E-TM-10-25 Standard Data Model and Protocol