



GEA Tianjin / 中国民航大学中欧航空工程师学院

CS41: VERIFICATION & VALIDATION









GEA Tianjin / 中国民航大学中欧航空工程师学院

SYSTEM ENGINEERING

Introduction





Systems

Integrated systems

Control-command

Telecommunication

Air Traffic Control

Millau viaduct

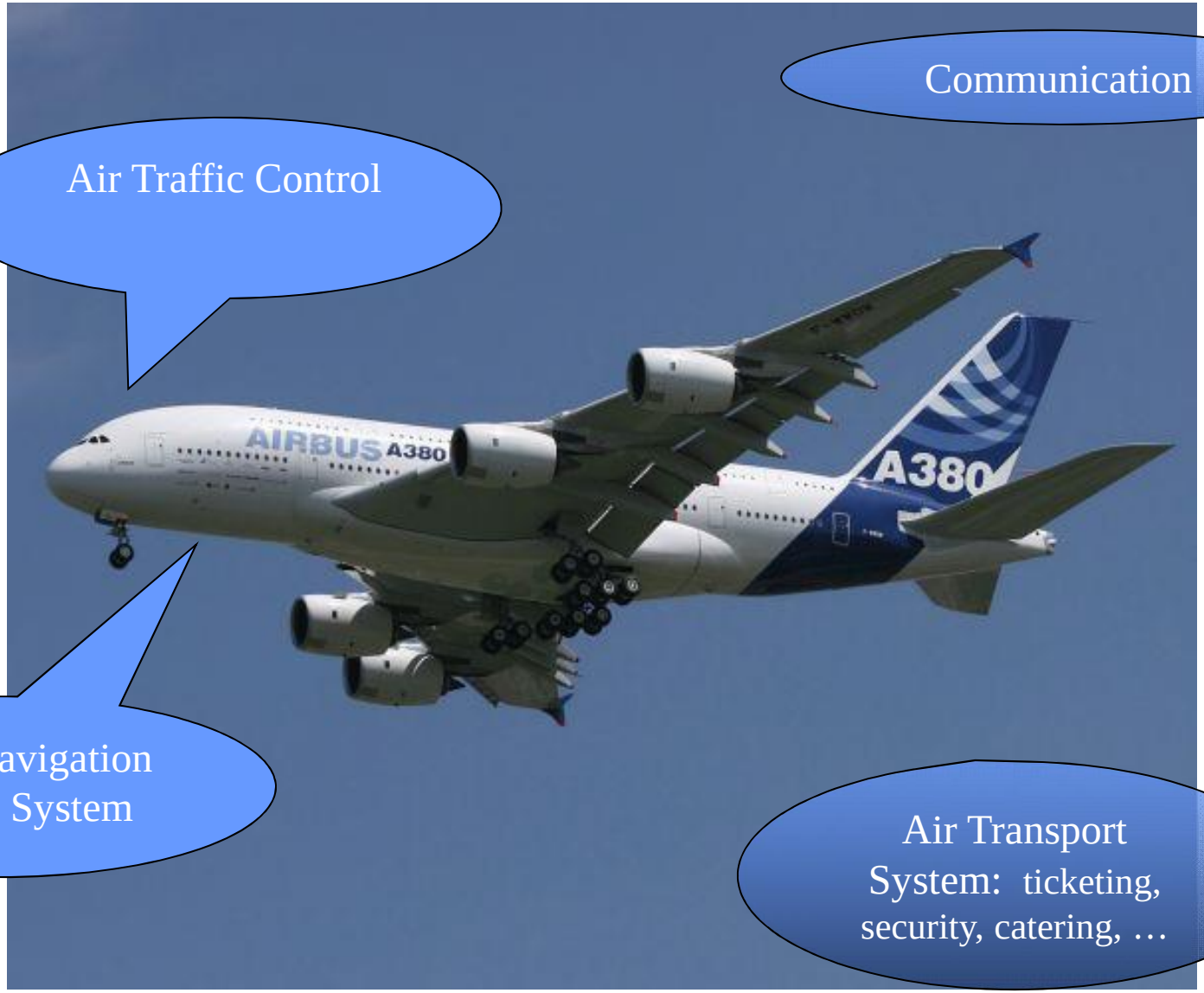
Towards nanosystems…

Systems thinking is applicable to all processes

Product = System of Interest+Enabling Systems

(Source: Airbus Product Development Process)

A system is always a sub-system of another system



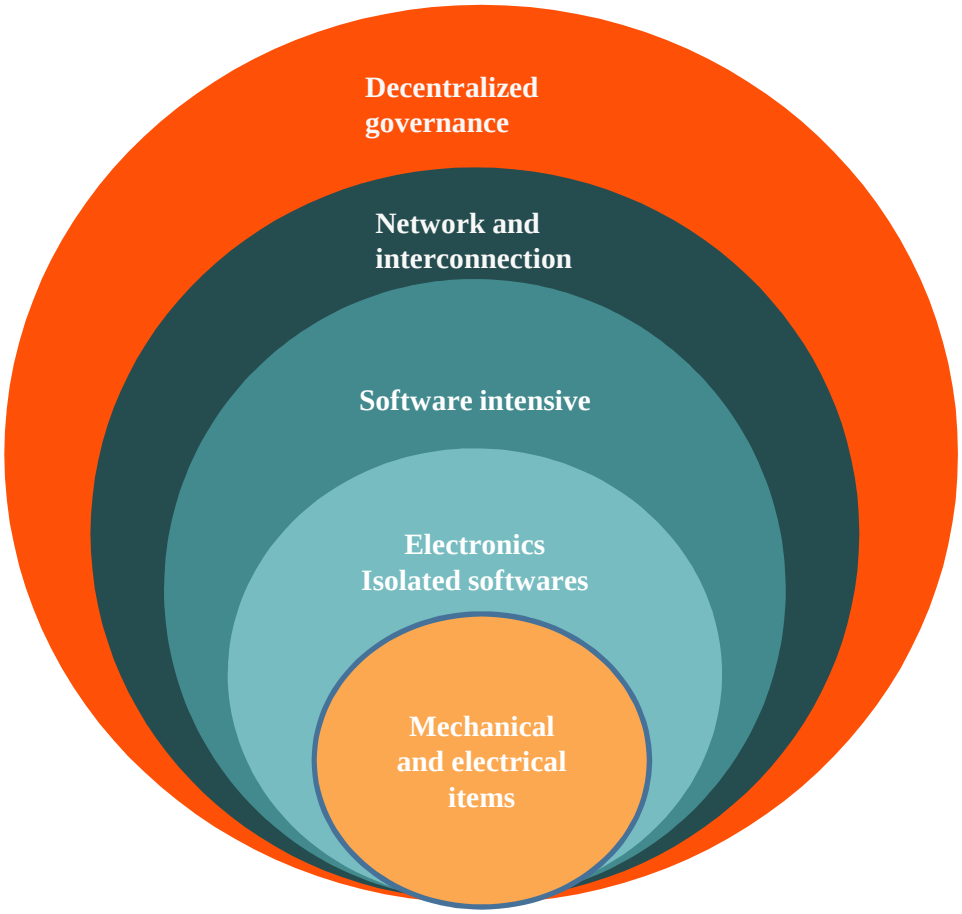
Systems Hierarchy

Complexity

Ambiguity

Lack of control

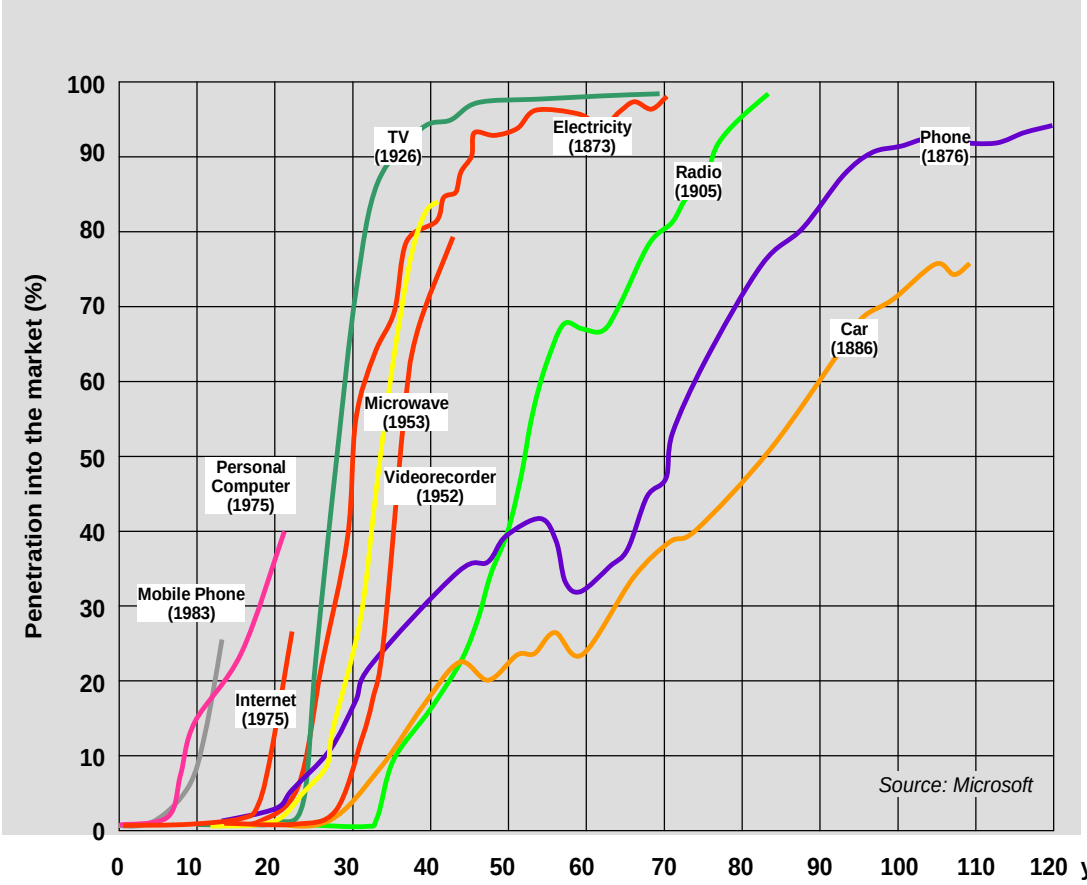
Systems of systems



(Source: INCOSE SE Vision 2025)

Engineering of systems: going faster

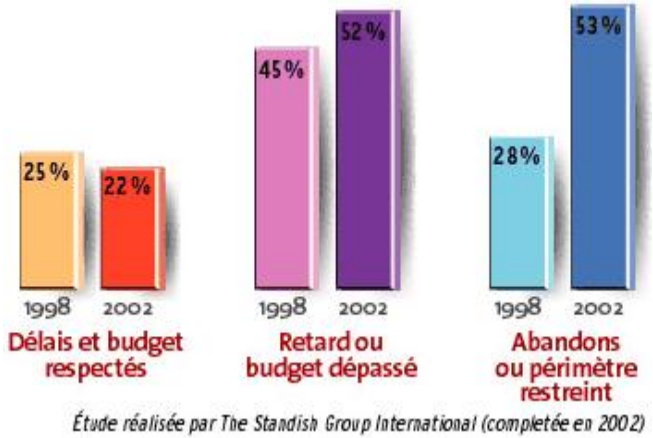
- **In the last century, the time from prototype to significant market penetration is dramatically reduced**



Evaluation of Engineering

- Over 30% of all software projects are cancelled before completion
- Over 70% of the remainder fail to deliver expected features
- The average project runs 189% over budget and overshoots its schedule by 222%

CHAOS, The Standish Group International, Inc., study published in 1994

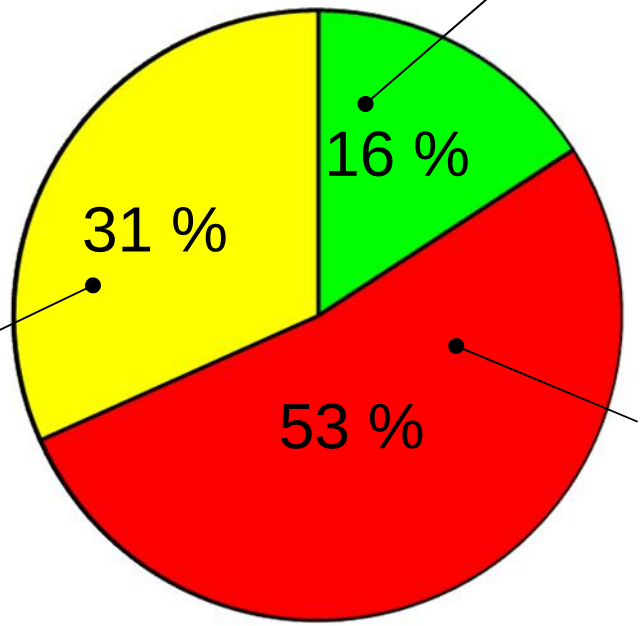


The Standish Group International (2002)
Source http://www.01net.com/article/212560.html

- Budget and Schedule over-shoot
- Fail to deliver the “right” system that works “right

The Chaos Report (1994)

US Standish Group survey based on 365 respondents represented 8,380 IT applications



Success:

The project is completed on-time and on-budget, with all features and functions as initially specified.

Impaired:

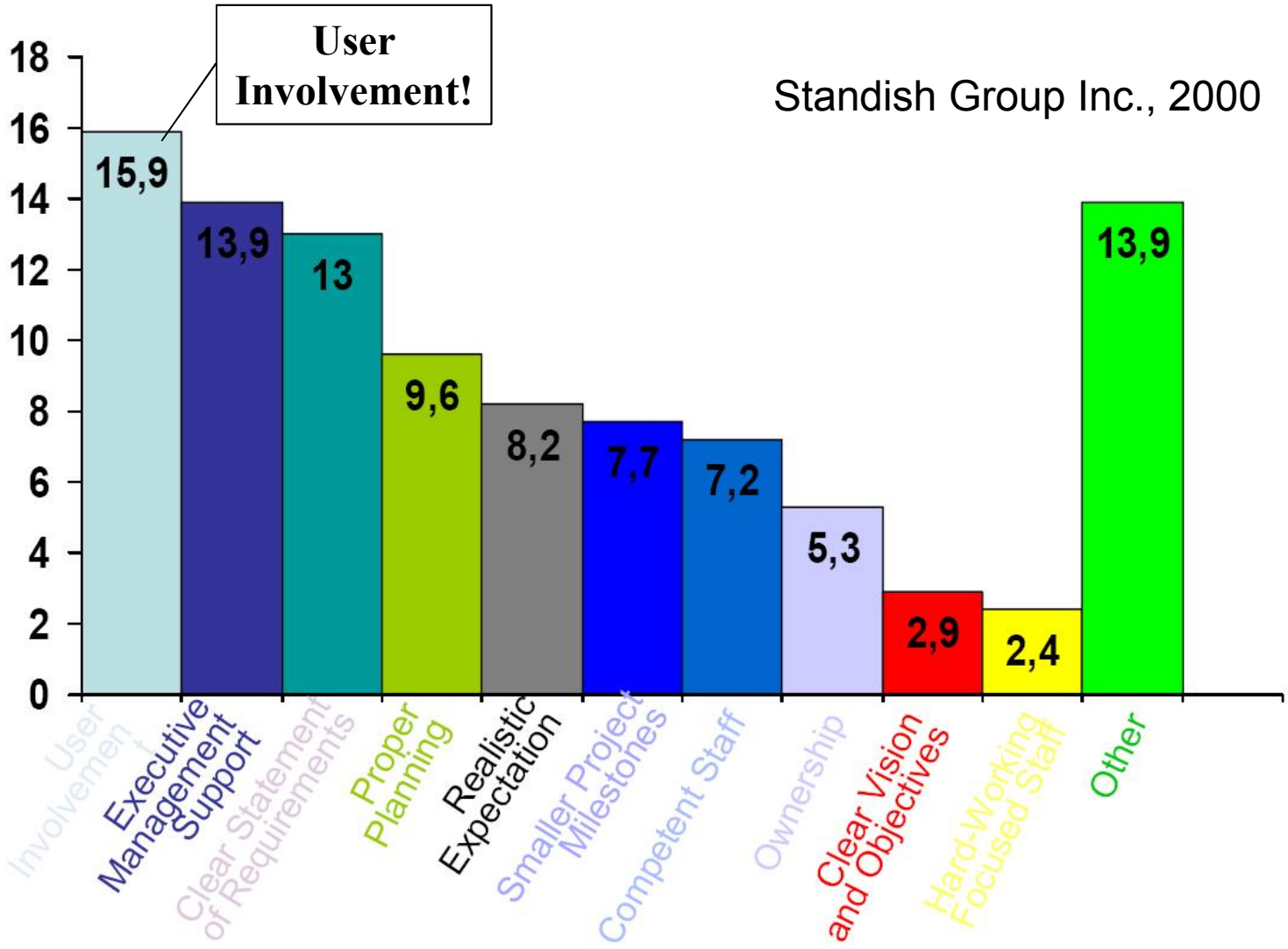
The project is cancelled at some point during the development cycle.

Challenge:

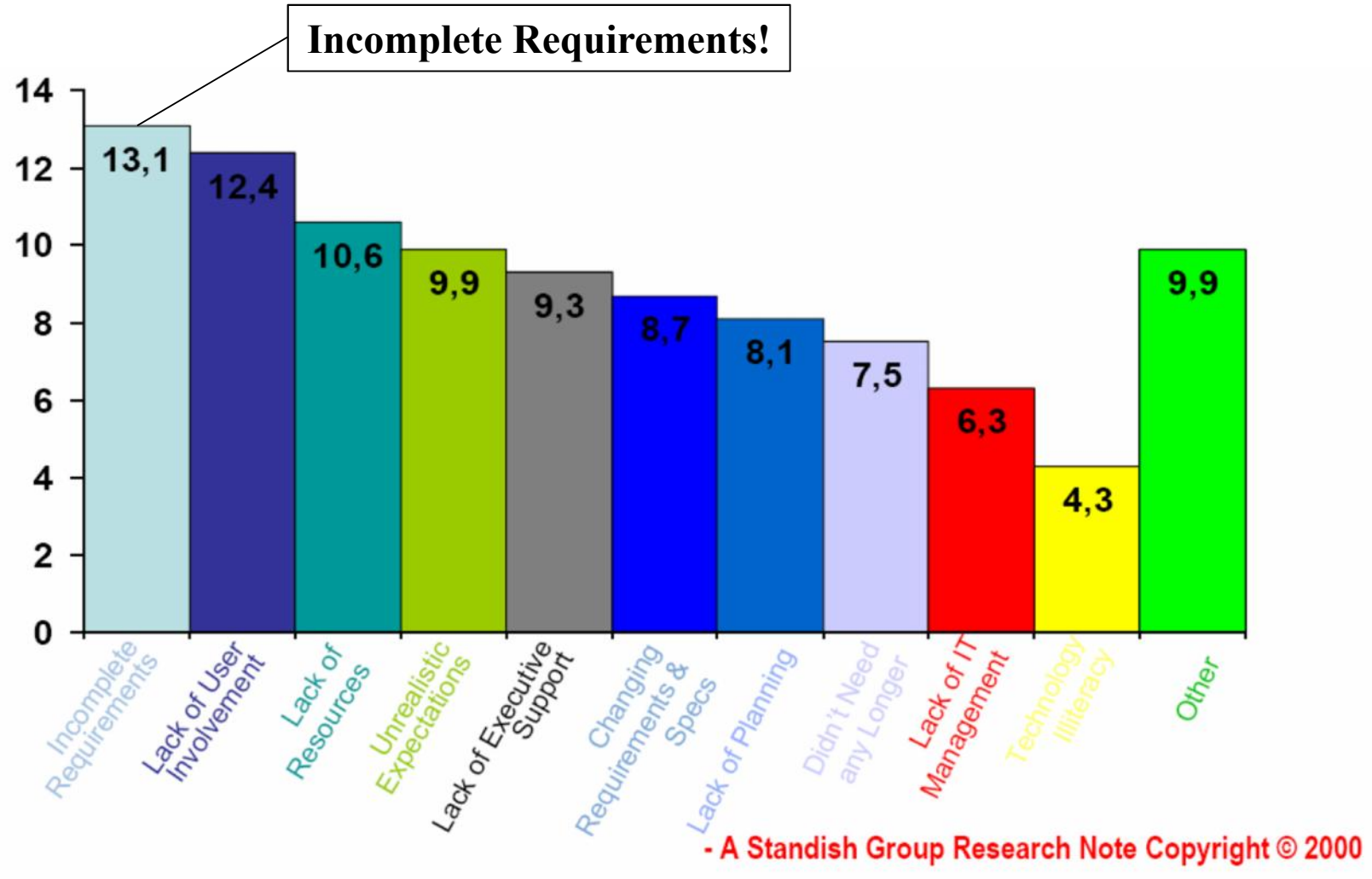
The project is completed and operational but over-budget, over the time estimate, and offers fewer features and functions than originally specified.

www.standishgroup.com

Success Factors



Problem Causes



Bigger and bigger systems

Watch	2 K instructions
Mobile phone	150 K instructions
Car	1 M instructions
Phone call center	1 M instructions
Linux kernel	3,7 M instructions
Combat Management System of the Charles de Gaulle	8 M instructions
Yahoo	11 M instructions
Windows 95	10 M instructions
Windows NT	16,5 M instructions
Windows 2000, XP	30 à 50 M instructions
Direction générale de la comptabilité publique (Bercy)	160 M instructions Cobol
Catia	200 M instructions ?





GEA Tianjin / 中国民航大学中欧航空工程师学院

SYSTEM ENGINEERING BASICS





What is a system ?

"A system is a combination of interacting elements organized to achieve one or more stated purposes " [ISO-15288:2008]

- A system element is a discrete part of a system that can be implemented to fulfil specified requirements.
- A system element can be hardware, software, data, humans, processes (e.g., processes for providing service to users), procedures (e.g., operator instructions), facilities, materials, and naturally occurring entities (e.g., water, organisms, minerals), or any combination.

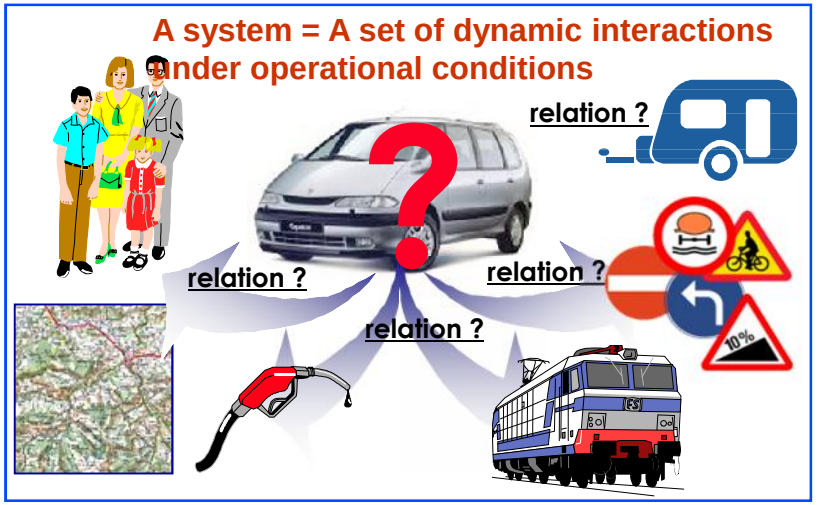
- « … combination of elements … » → architectures
- « … interacting elements … » →interfaces, behaviours
- « … stated purposes » → why does this system exist ? What is it for ?

"System": Fundamentals

The term "system" was used in the past in philosophy and metaphysics ;
It was the source of the "systemic" approach.

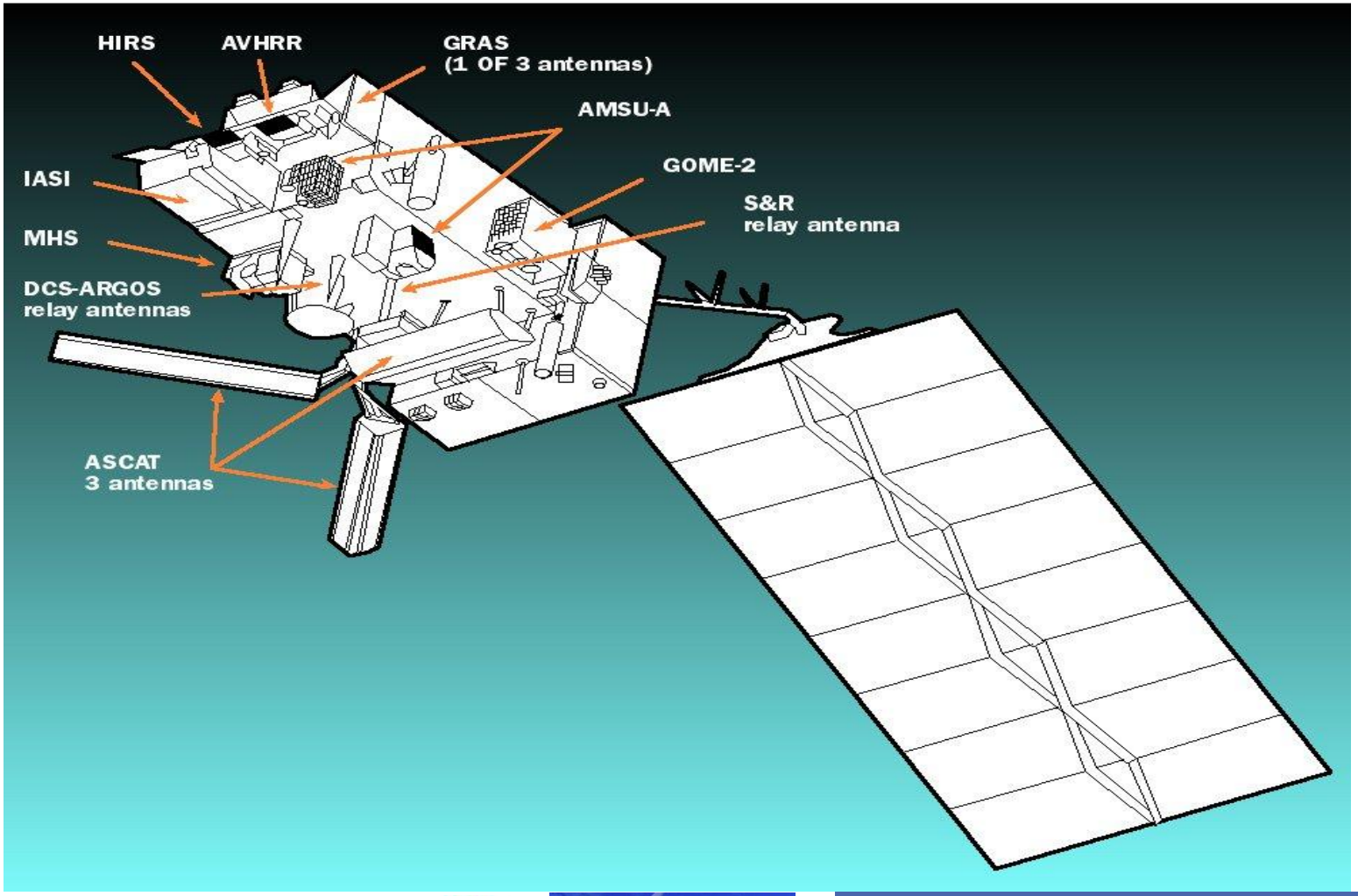
- Nowadays, systemic focuses on
  - The General Theory of Systems (generic model of the world and its phenomena)
  - Methods to model abstract complex products

- System Engineering is twofold and addresses
  - System vision of products / services
  - Basic Models and Generic Processes for modeling



System example

- A satellite is composed of systems



Systems within a System

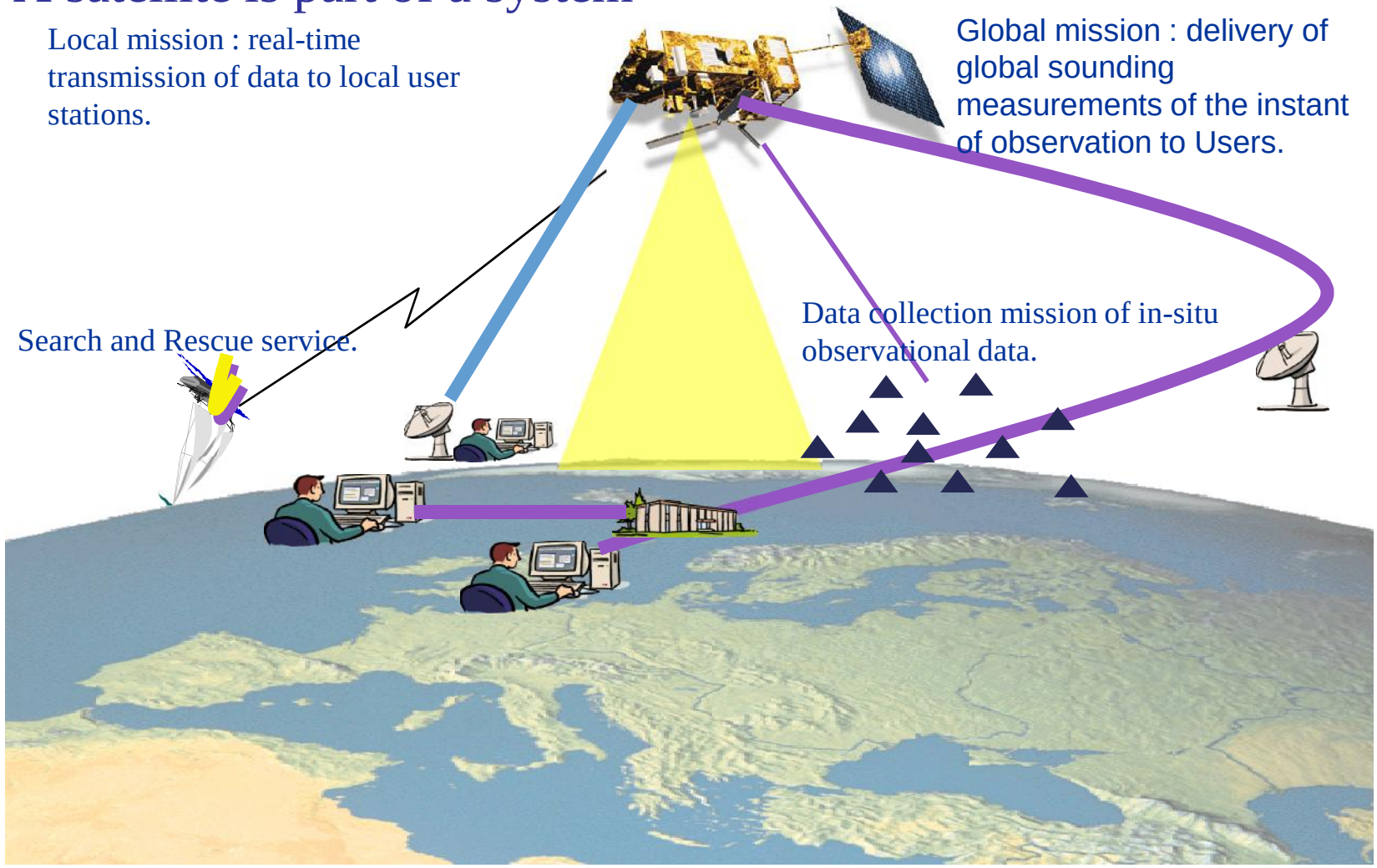
- A satellite is part of a system

Local mission : real-time transmission of data to local user stations.

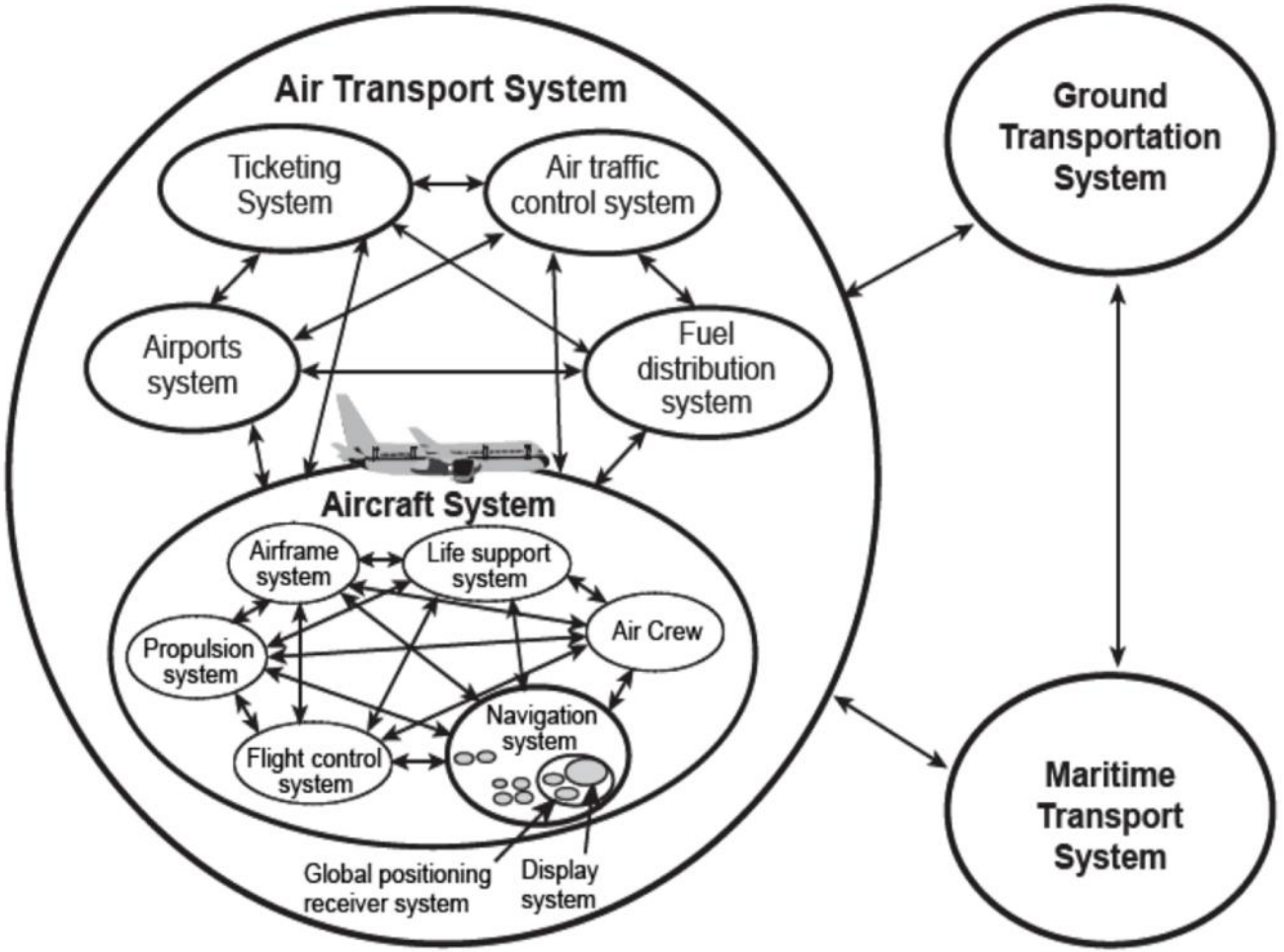
Global mission : delivery of global sounding measurements of the instant of observation to Users.

Search and Rescue service.

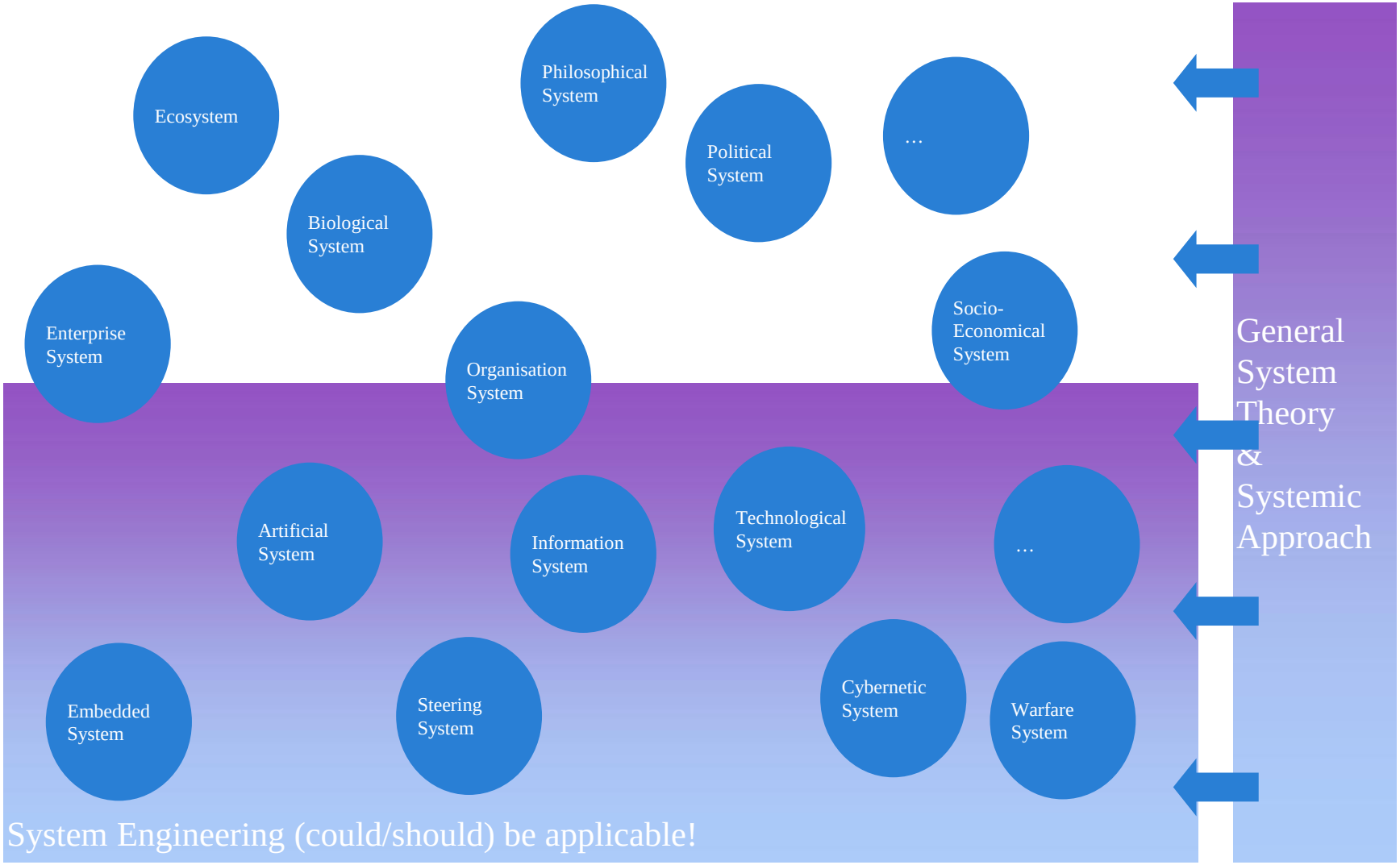
Data collection mission of in-situ observational data.



Systems of Systems



A galaxy of systems



What System Engineering allows to anticipate

Systems engineering?

System Engineering is a interdisciplinary approach,

integrating all specialities in a teamwork

using a structured specification and design process

encompassing the whole life-cycle of the system.

This approach takes into account the constraints of the market, the needs of the customer and the industrial know-how.

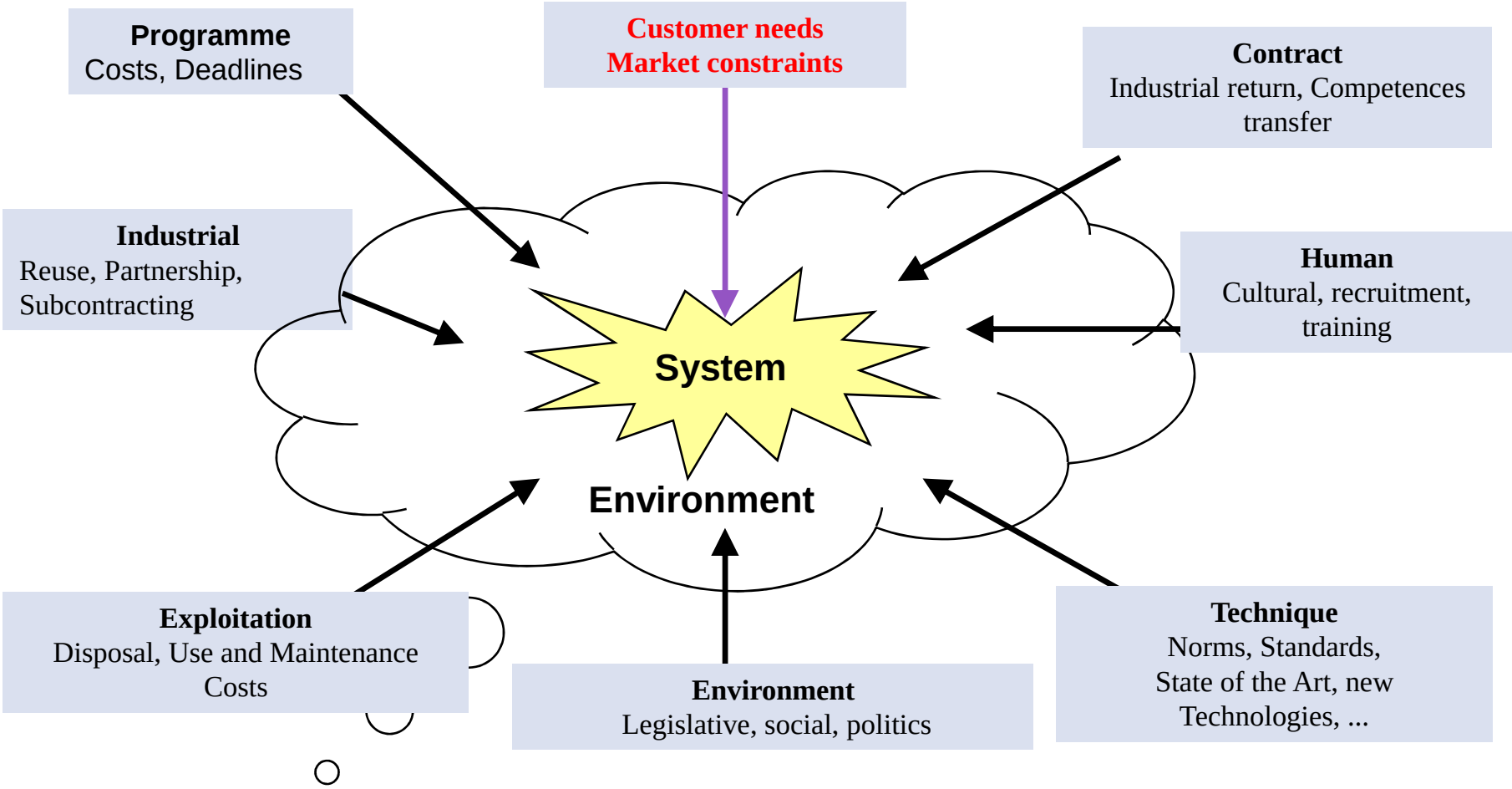
Systems Engineering per EIA/IS632

Systems engineering is "an interdisciplinary approach encompassing the entire technical effort to evolve and verify an integrated and life-cycle balanced set of system people, product, and process solutions that satisfy customer needs. Systems engineering encompasses (a) the technical efforts related to the development, manufacturing, verification, deployment, operations, support) disposal of, and user training for, system products and processes; (b) the definition and management of the system configuration; (c) the translation of the system definition into work breakdown structures; and (d) development of information for management decision making."

System Engineering per NASA

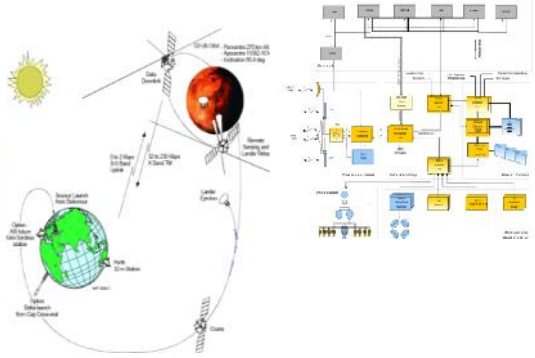
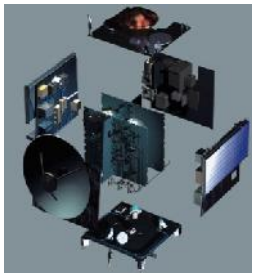
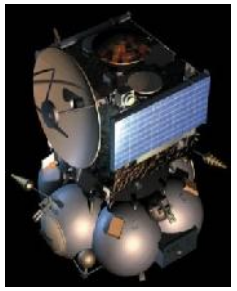
Systems engineering is a robust approach to the design, creation, and operation of systems. In simple terms, the approach consists of identification and quantification of system goals, creation of alternative system design concepts, performance of design trades, selection and implementation of the best design, verification that the design is properly built and integrated, and post-implementation assessment of how well the system meets (or met) the goals. The approach is usually applied repeatedly and recursively, with several increases in the resolution of the system baselines (which contain requirements, design details, verification procedures and standards, cost and performance estimates, and so on).

Integrate all the constraints

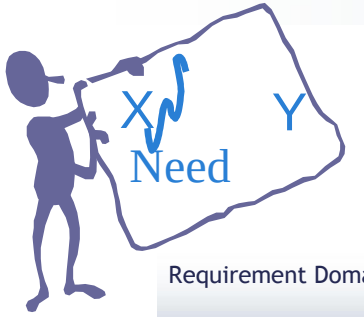


From the dream …

… up to fulfilment!


idea … mission … mock-up, models, concept … cad, digital mock-up …. Concrete Product



System Engineering → Optimised Solution

MULTI Disciplinary

Requirement Domain

Client economic area,
Usage, exploitation

Skill Domain

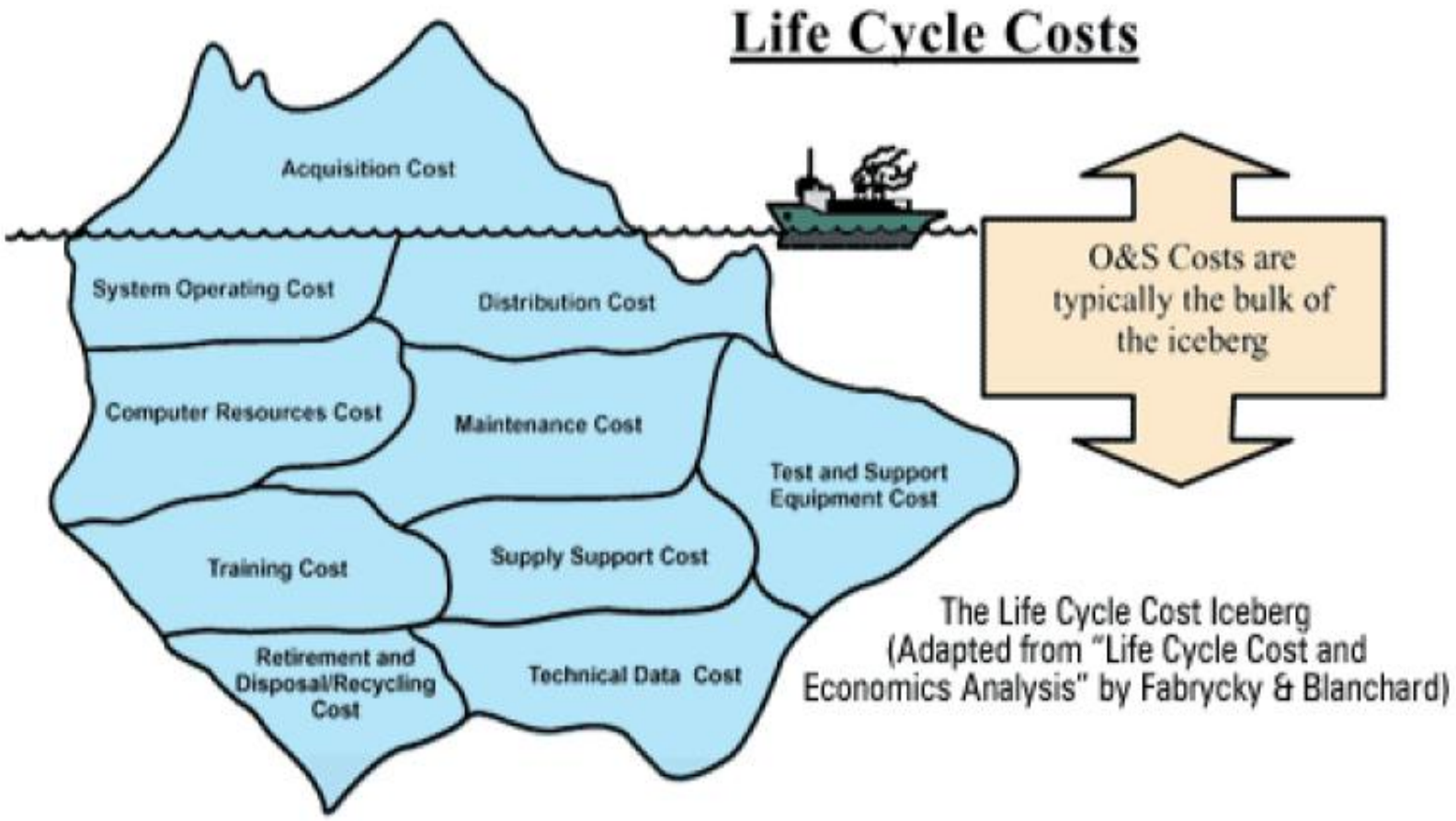
Mechanics
Electrical
Software
…

Transversal Domain

Quality
Dependability
Safety
Ergonomics, Human factors,

Support and Training Domain

Supply
Production
Exploitation
Maintenance
Retirement



+ “deep” hidden cost. For example, over-cost due to a poor or loss of effectiveness

Relationship between System Engineering and Project Management

Project Management

Handling the contract Organize

- Acceptance criteria
- Project&Industrial Organisation
- Make or Buy
- Suppliers Selection & Control
- Identification of competencies
- Planning, milestones, critical path
- Task launching and control

System Engineering

Optimize the Solution

- Right definition of necessary functions& interfaces
- Architectures
- Reused Components, COTS
- Identification of Technical solution
- Industrial Constraints

- Coverage of Needs
- Compliance to performances
- Coverage of the full life-cycle

Les Responsabilités GP & IS

➢ Responsabilités de la Gestion de Projet

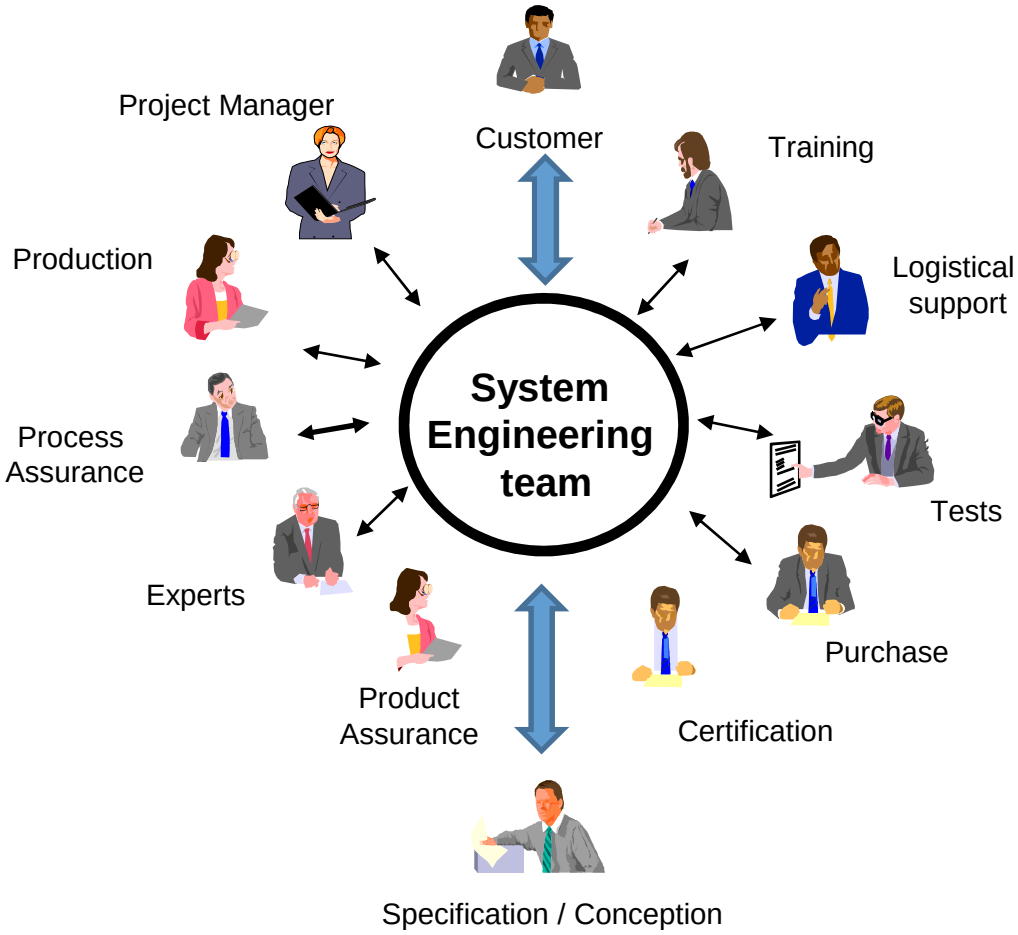
Gestion de Projet

- **Relations avec le Client**
  - États d'avancement du projet
  - Obligation du Client
  - Équipements Fournis par le Client
  - Fournitures (attendues, réalisées, prévues)

- **Gestion et Contrôle du Projet:**
  - Coût, Planning et Organisation,
  - Décisions et Justifications,
  - Actions Correctives, (incluant les aspects Assurance Produit)
  - Configuration et Data management,
  - Identification, gestion et contrôle des Risques.

Actors of System Engineering

System Engineering team within a company



The system Engineering team is at the core of the company activities oriented towards the product.





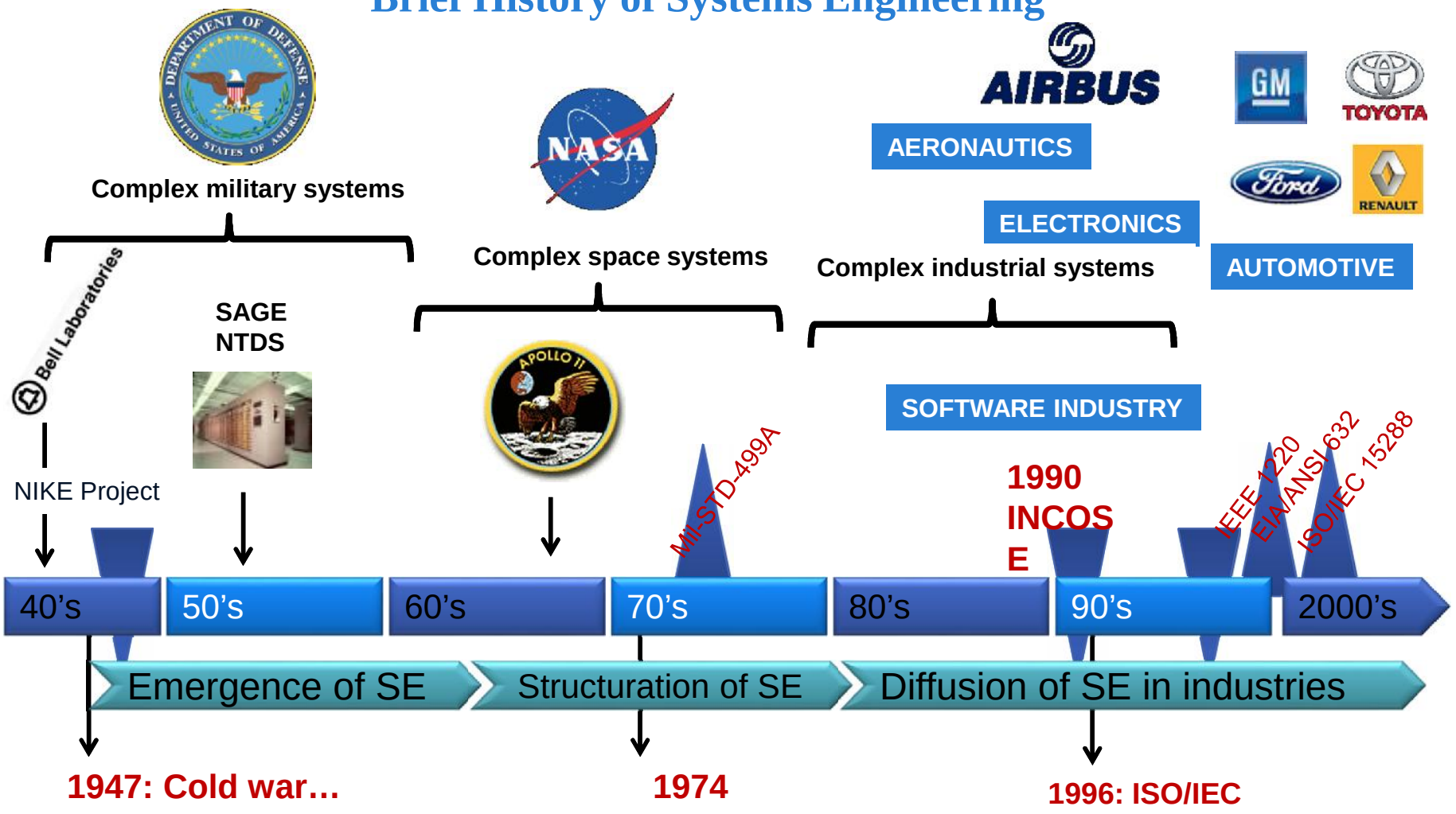
GEA Tianjin / 中国民航大学中欧航空工程师学院

SYSTEM ENGINEERING FUNDATIONS





Brief History of Systems Engineering



Origin of the current SE Standards

Standard for Application and Management of the Systems Engineering Process

IEEE 1220 Trial Use 94 → IEEE 1220 January 99

System Engineering

Mil-STD-499A Mai 1974 → Mil-STD-499B June 1992 coordination copy

The US Perry directive puts an end to the new US military standards in June 1994

Processes for Engineering a System

EIA/IS 632 December 94 → EIA/ANSI 632 January 99

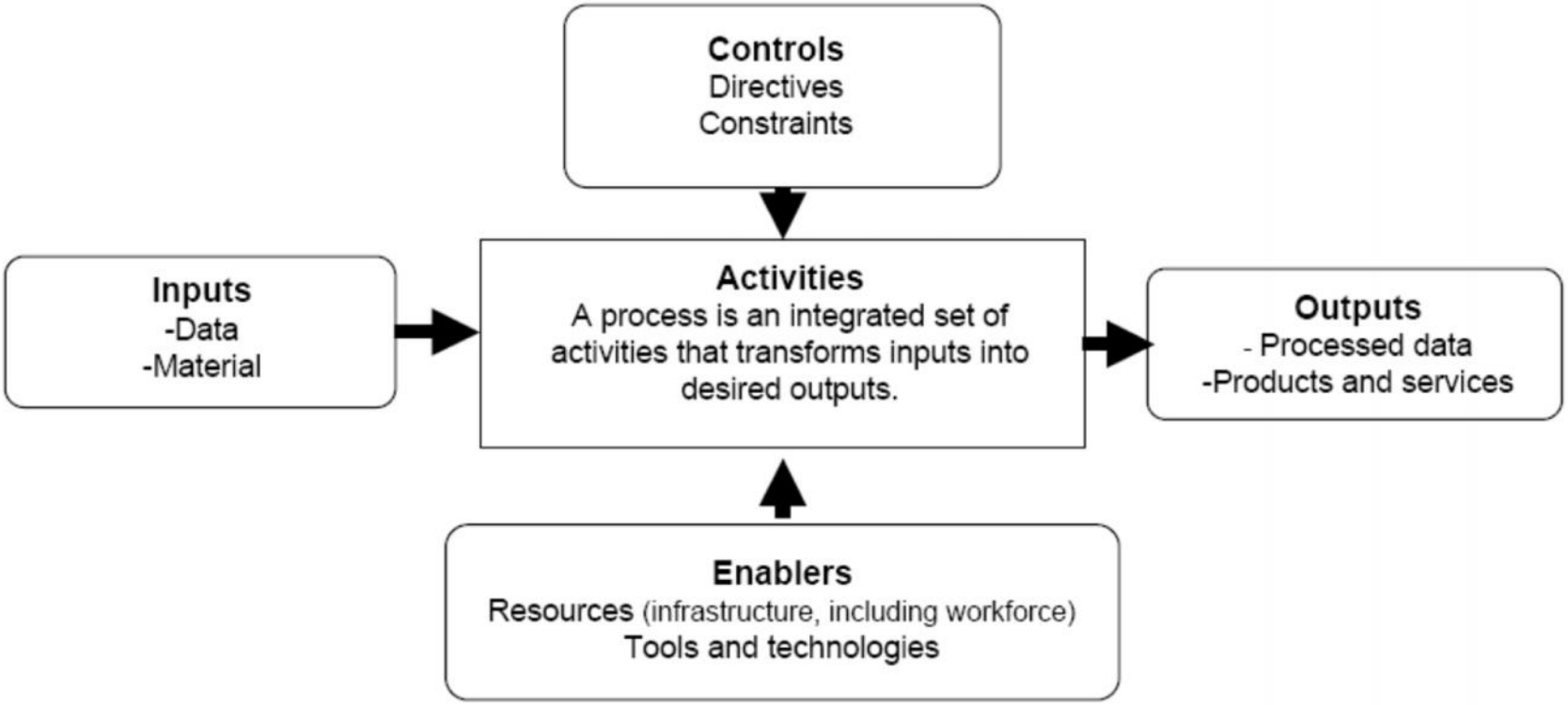
Coordination

ISO/IEC 12207 2008

Software life cycle processes

System life cycle processes

ISO/IEC 15288 December 96 → ISO/IEC 15288 October 2002 → ISO/IEC 15288 February 2008



A process transform inputs into outputs by bringing value added using means and resources

[INCOSE HDBK]

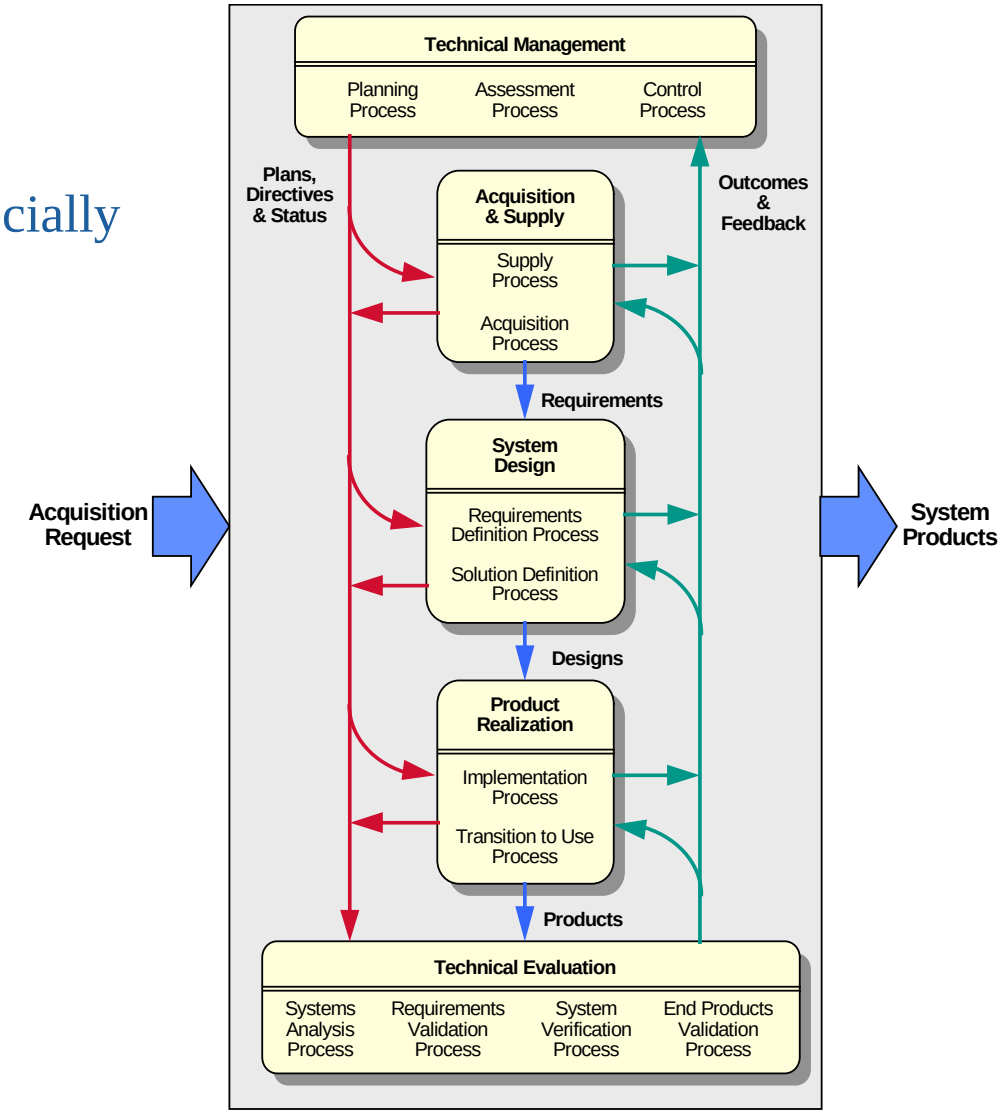
And not « document production » oriented

EIA632: main Systems Engineering processes

➢ANSI/EIA-632

- Used by major industrials, especially in aeronautics and space

- 5 main Processes
  - 13 Sub-Processes
    - 33 Requirements



EIA632: Sub-processes and requirements

SUPPLY PROCESS REQUIREMENTS

1—Product Supply

ACQUISITION PROCESS REQUIREMENTS

2—Product Acquisition

3—Supplier Performance

PLANNING PROCESS REQUIREMENTS

4—Process Implementation Strategy

5—Technical Effort Definition

6—Schedule and Organization

7—Technical Plans

8—Work Directives

ASSESSMENT PROCESS REQUIREMENTS

9—Progress Against Plans and Schedules

10—Progress Against Requirements

11—Technical Reviews

CONTROL PROCESS REQUIREMENTS

12—Outcomes Management

13—Information Dissemination

REQUIREMENTS DEFINITION PROCESS REQUIREMENTS

14—Acquirer Requirements

15—Other Stakeholder Requirements

16—System Technical Requirements

SOLUTION DEFINITION PROCESS REQUIREMENTS

17—Logical Solution Representations

18—Physical Solution Representations

19—Specified Requirements

IMPLEMENTATION PROCESS REQUIREMENTS

20—Implementation

TRANSITION TO USE PROCESS REQUIREMENTS

21—Transition to Use

SYSTEMS ANALYSIS PROCESS REQUIREMENTS

22—Effectiveness Analysis

23—Tradeoff Analysis

24—Risk Analysis

REQUIREMENTS VALIDATION PROCESS REQUIREMENTS

25—Requirement Statements Validation

26—Acquirer Requirements Validation

27—Other Stakeholder Requirements Validation

28—System Technical Requirements Validation

29—Logical Solution Representations Validation

SYSTEM VERIFICATION PROCESS REQUIREMENTS

30—Design Solution Verification

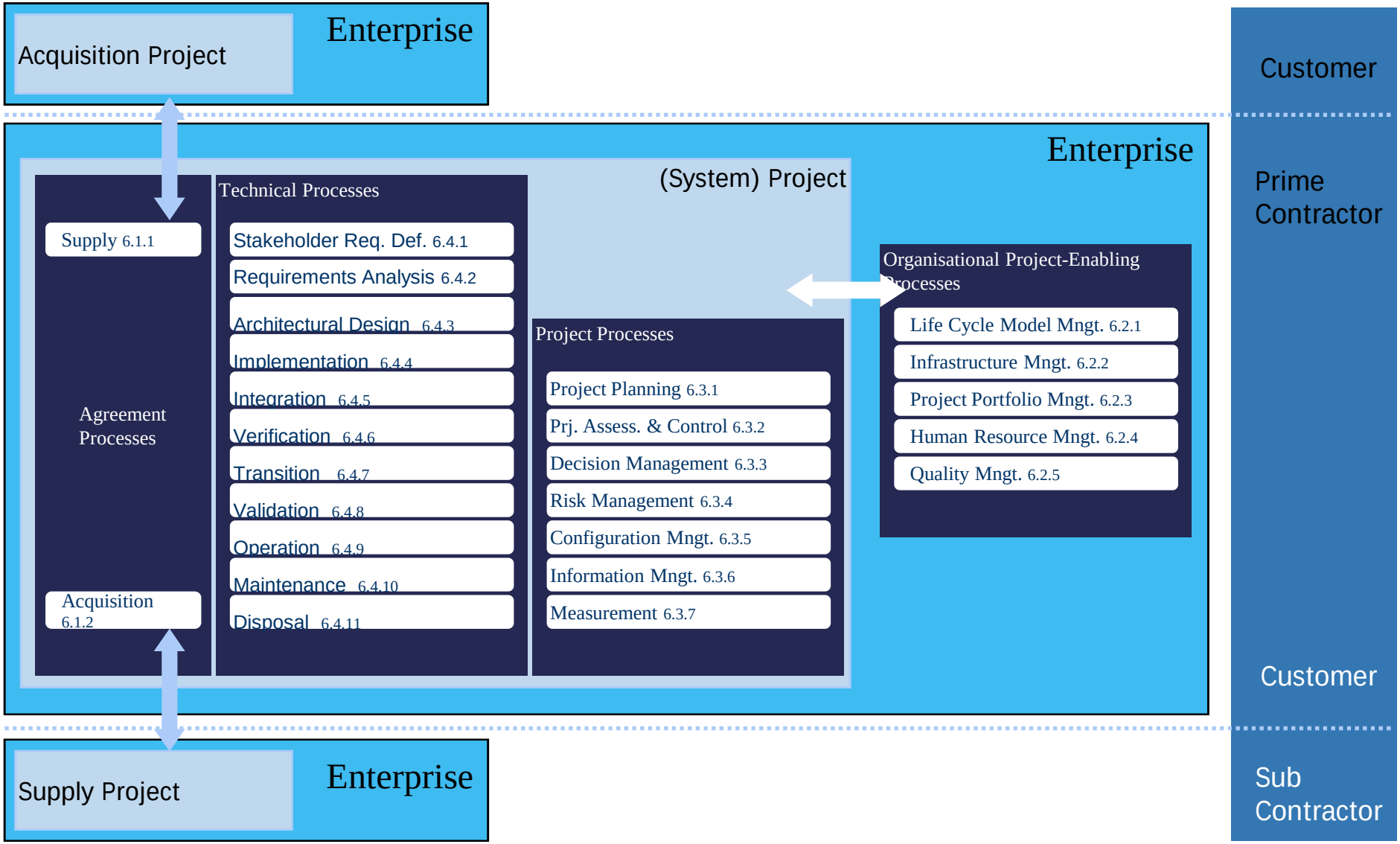
31—End Product Verification

32—Enabling Product Readiness

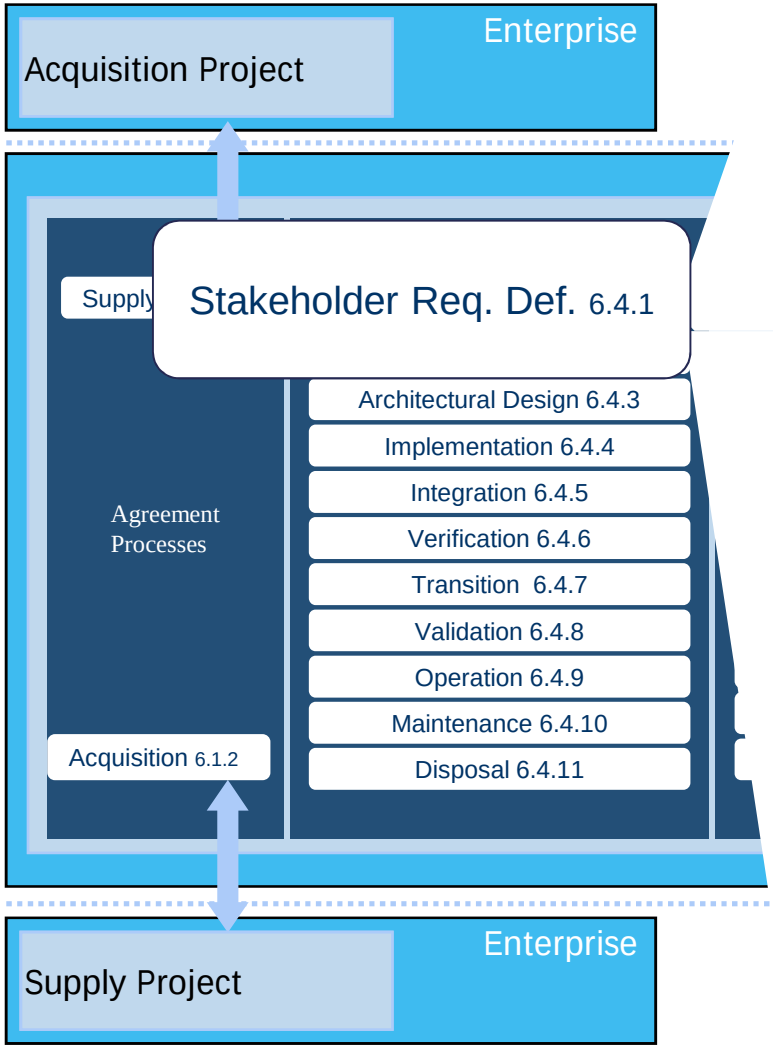
END PRODUCTS VALIDATION PROCESS REQUIREMENTS

33—End Products Validation

ISO 15288 Processes: Processes to be used to engineer a system



ISO 15288



6.4.1 Stakeholder Requirements Definition Process

6.4.1.1 Purpose

The purpose of the Stakeholder Requirements Definition Process is to define the requirements for a system that can provide the services needed by users and other stakeholders in a defined environment.

…

6.4.1.2 Outcomes

…

c) Traceability of stakeholder requirements to stakeholders and their needs is achieved.
d) The stakeholder requirements are defined.
e) Stakeholder requirements for validation are identified.

6.4.1.3 Activities and tasks

a) Elicit stakeholder requirements

1) Identify the individual stakeholders …

b) **Define stakeholder requirements**

…

c) **Analyze and maintain stakeholder requirements**

…

Sub Contractor

INCOSE

- 7000 members,
- Present in 100+ countries

"Share, promote and advance the best of systems engineering from across the globe for the benefit of humanity and the planet"

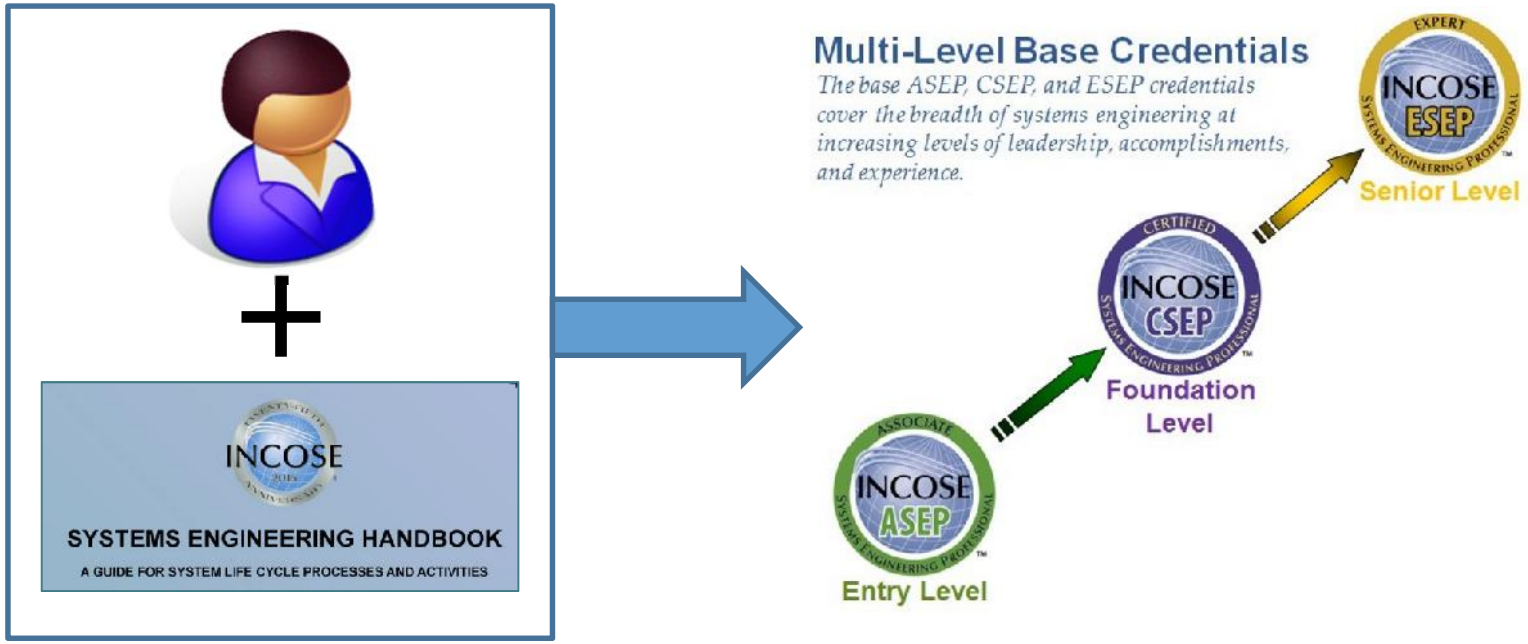
www.incose.org

- Prospective (*SE Vision 2025*)
- Journals and newsletters(*Insight, System Engineering Journal)*,
- Knowledge base (*SE Body Of Knowledge*)
- Practices and techniques (*SE Handbook, various* guides)
- International workgroups

INCOSE events

- Annual symposium
  - Hundreds of participants

- Certification program for individuals



AFIS

Association Française d'Ingénierie Système

INCOSE AFFILIATE

- 8 Technical committees
  - Publication of guides and best practices
- Organization of national events
  - Annual conference
  - Students' competition (Rob'AFIS)
  - Technical days
- Regional chapters (Ex : Midi-Pyrénées)

GEA Tianjin / 中国民航大学中欧航空工程师学院

AERONAUTICAL CONTEXT

Recommended practices for certification

Certification organizations

- 2 main organizations responsible of the delivery of compliance attestation (airworthiness certificate):
  - EASA (Europe) : European Aviation Safety Agency
    - Founded in 2003, Headquarter : Cologne, Germany
  - FAA (USA) : Federal Aviation Administration
    - Founded in 1958, Headquarter : Washington DC, USA

    ⇒ FAR : Federal Aviations Regulations

- Some countries have their own organizations:
  - China (CAAC) , Canada (TC), Japan (JCAB), Brazil (CTA), Russia (AAR) ...

Certification Basis

Part 21 : Certification of Aircraft & Related Products, Parts & Appliances

CS 25 : Certification Specifications for Large Aeroplanes

CS 25.1309 : Equipment, Systems & Installations

AMC 25.1309 : System Design & Analysis

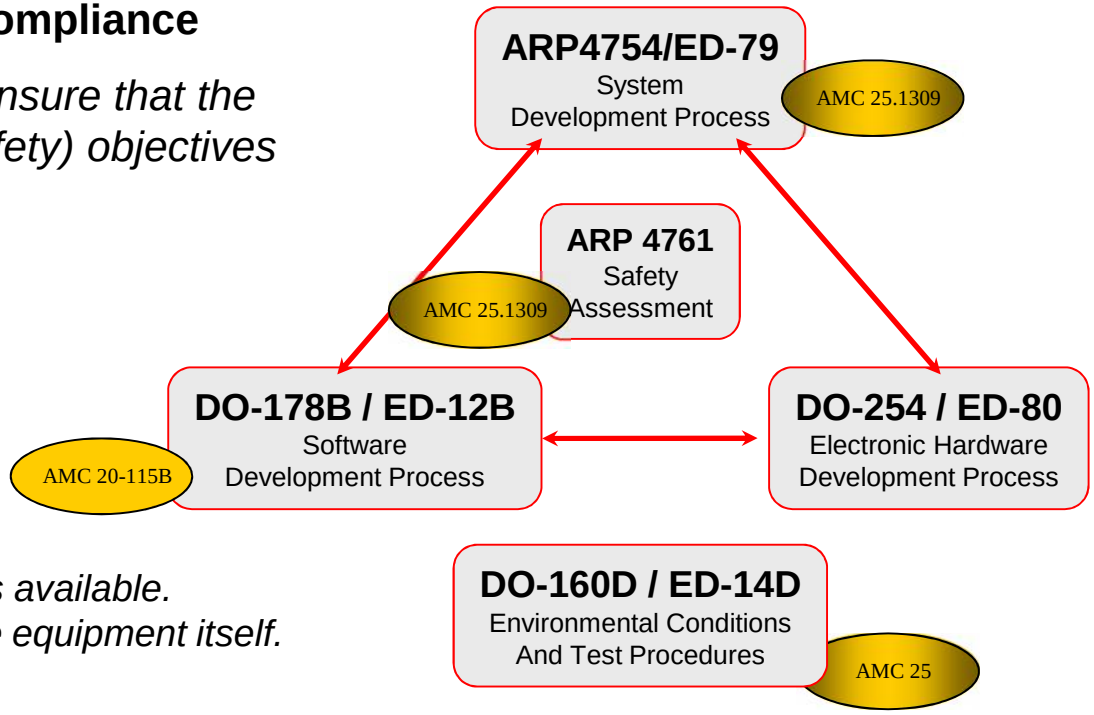
AMC 20: General Acceptable Means of Compliance for Airworthiness of Products, Parts and Appliance

Airworthiness Standards

Set of requirements to ensure passengers' safety

Acceptable Means Of Compliance

A structured approach to ensure that the equipment will meet the (safety) objectives



The equipment is available.
Tests are applied on the equipment itself.

Criticity Level Definition (DAL) and Activity Impacts

- Based on statistics, most of severe accidents (loss of aircraft, passenger or crew death), world wide rate is 1 per million of flight hours
- Only 10 percent of fatal accidents have been attributed to a critical failure conditions involving aircraft systems
- There are approximately 100 catastrophic failure conditions

Criticity Level Definition (DAL) and Activity Impacts

- To prevent a deterioration of current fatal rate, the probability of occurrence of each catastrophic failure conditions must be shown to be at most :
  - 10-6 x (0,1) x (0,01) = 10-9 per flight hour

- The certification criteria of CS 25.1309 is based on this fundamental safety target

Criticity Level Definition (DAL)

Effect on Aeroplane	No effect on operational capabilities or safety	Slight reduction in functional capabilities or safety margins	Significant reduction in functional capabilities or safety margins	Large reduction in functional capabilities or safety margins	Normally with hull loss
Effect on Occupants excluding Flight Crew	Inconvenience	Physical discomfort	Physical distress, possibly including injuries	Serious or fatal injury to a small number of passengers or cabin crew	Multiple fatalities
Effect on Flight Crew	No effect on flight crew	Slight increase in workload	Physical discomfort or a significant increase in workload	Physical distress or excessive workload impairs ability to perform tasks	Fatalities or incapacitation
Allowable Qualitative Probability	No Probability Requirement	<---Probable---->	<----Remote---->	Extremely <----------> Remote	Extremely Improbable
Allowable Quantitative Probability: Average Probability per Flight Hour on the Order of:	No Probability Requirement	<----------> $<10^{-3}$ Note 1	<----------> $<10^{-5}$	<----------> $<10^{-7}$	$<10^{-9}$
Classification of Failure Conditions	No Safety Effect	<-----Minor------>	<-----Major------>	<--Hazardous-->	Catastrophic

Design Assurance Level

- Design Assurance Level definition : Determines the level of rigor and discipline to develop an item
  - System
  - Hardware
  - Software
- Assignment of Equipment development assurance levels (DAL)
  - The Equipment development assurance level is assigned based on:
    - System development assurance level
    - Architecture Consideration
  - Rules for equipment DAL assignment are defined in ARP 4754

Assignment of system development assurance levels (DAL)

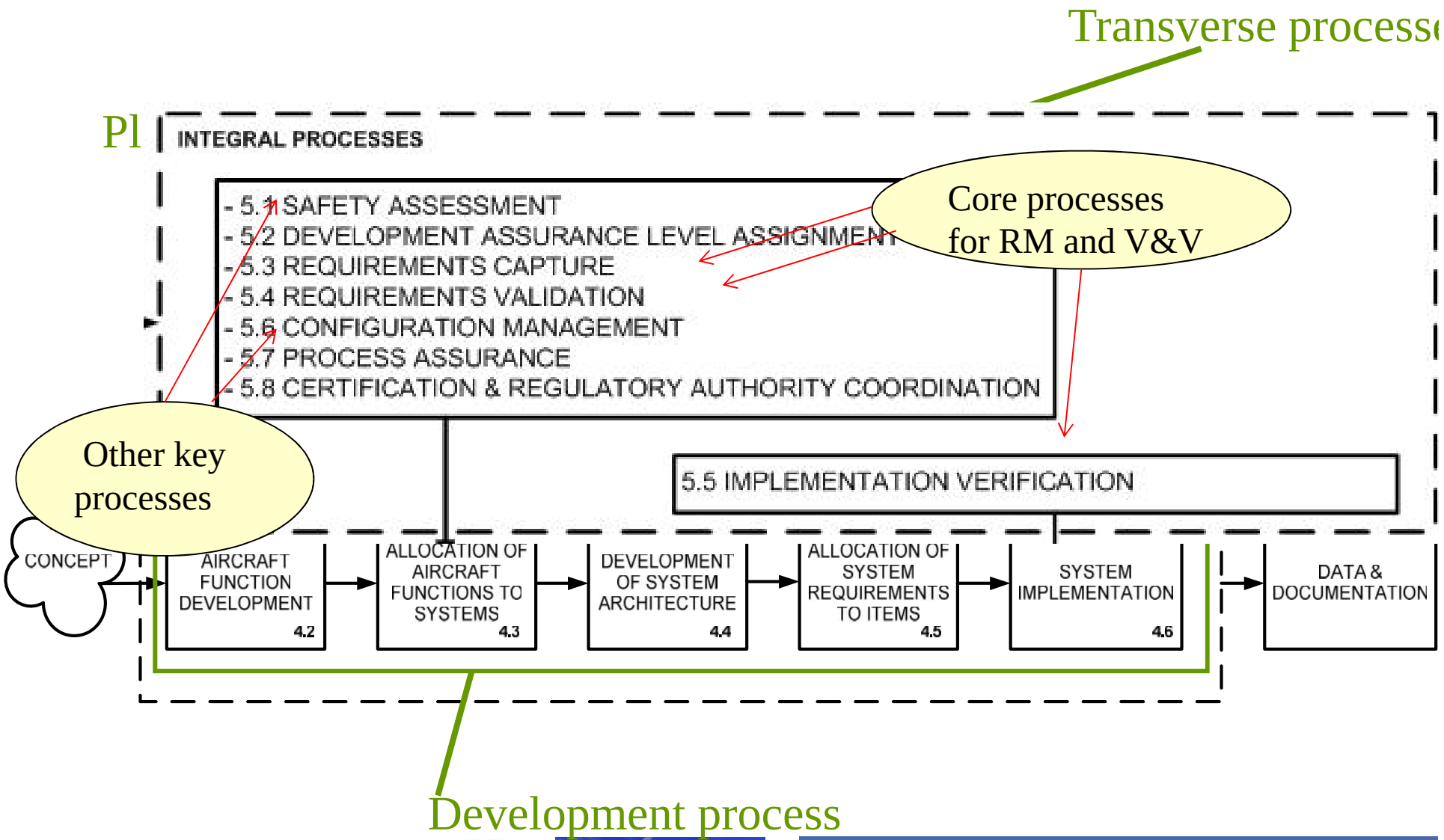
- The system development assurance level is assigned based on the most severe failure condition classification associated with the applicable aircraft level function

Failure condition classification	System Development Assurance level
Catastrophic	A
Hazardous	B
Major	C
Minor	D
No safety effect	E

Why ARP4754 ?

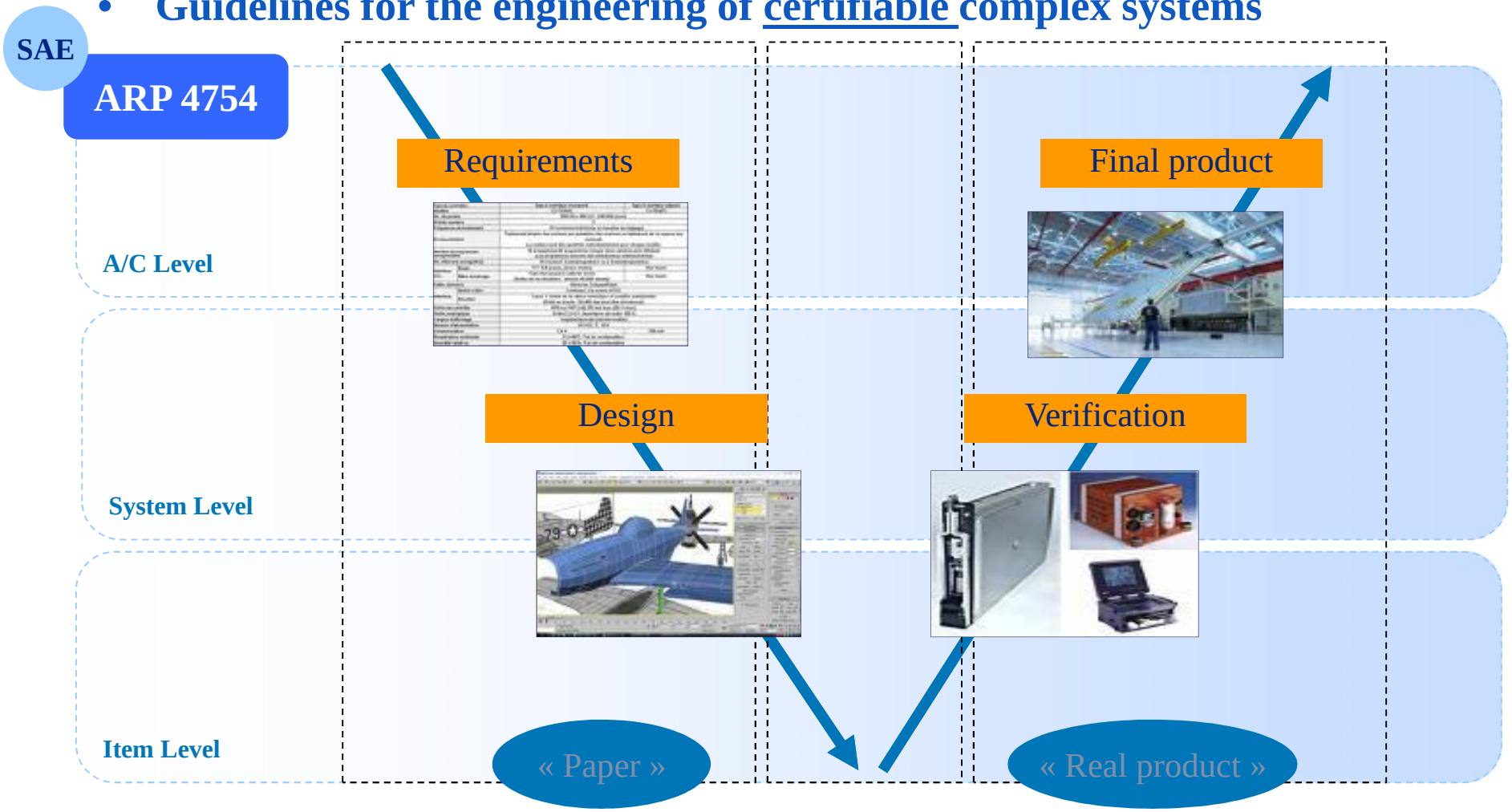
- Aircraft System Complexity increase
  - Design error increase
  - No possible exhaustive tests
  - Development assurance activities are needed to detect these errors through a structured development
- 3 Guides to manage development assurance
  - System level: ARP 4754
  - Hardware Level: DO 254
  - Software level: DO 178

ARP 4754A processes

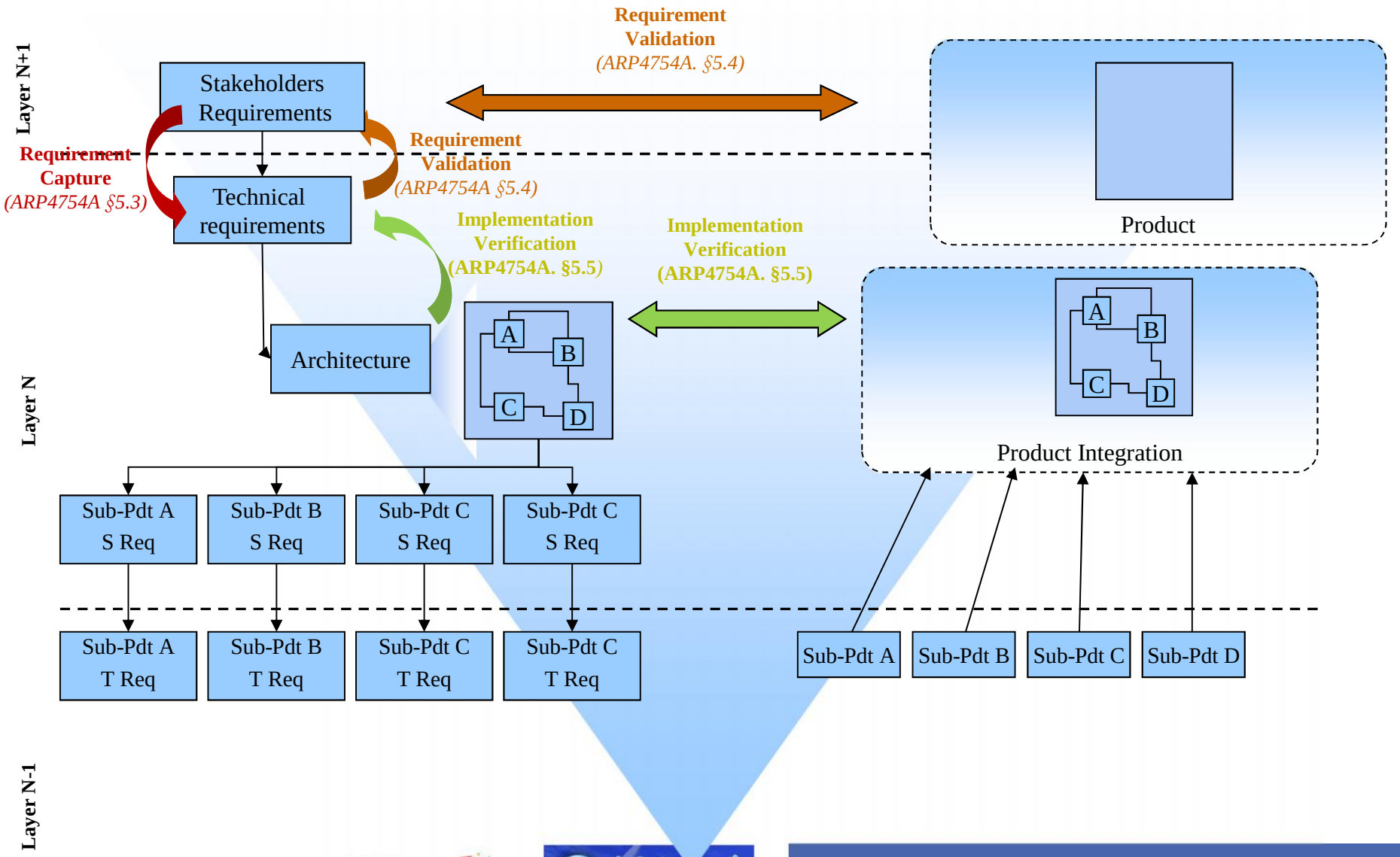


Development process driven by ARP4754A

- Guidelines for the engineering of certifiable complex systems



Certification-oriented engineering



Aim of ARP4754

- Provide Recommend Practices for engineering,
  → Not regulatory requirements, not mandatory

- Alternative practices may be used to obtain Certification

But …

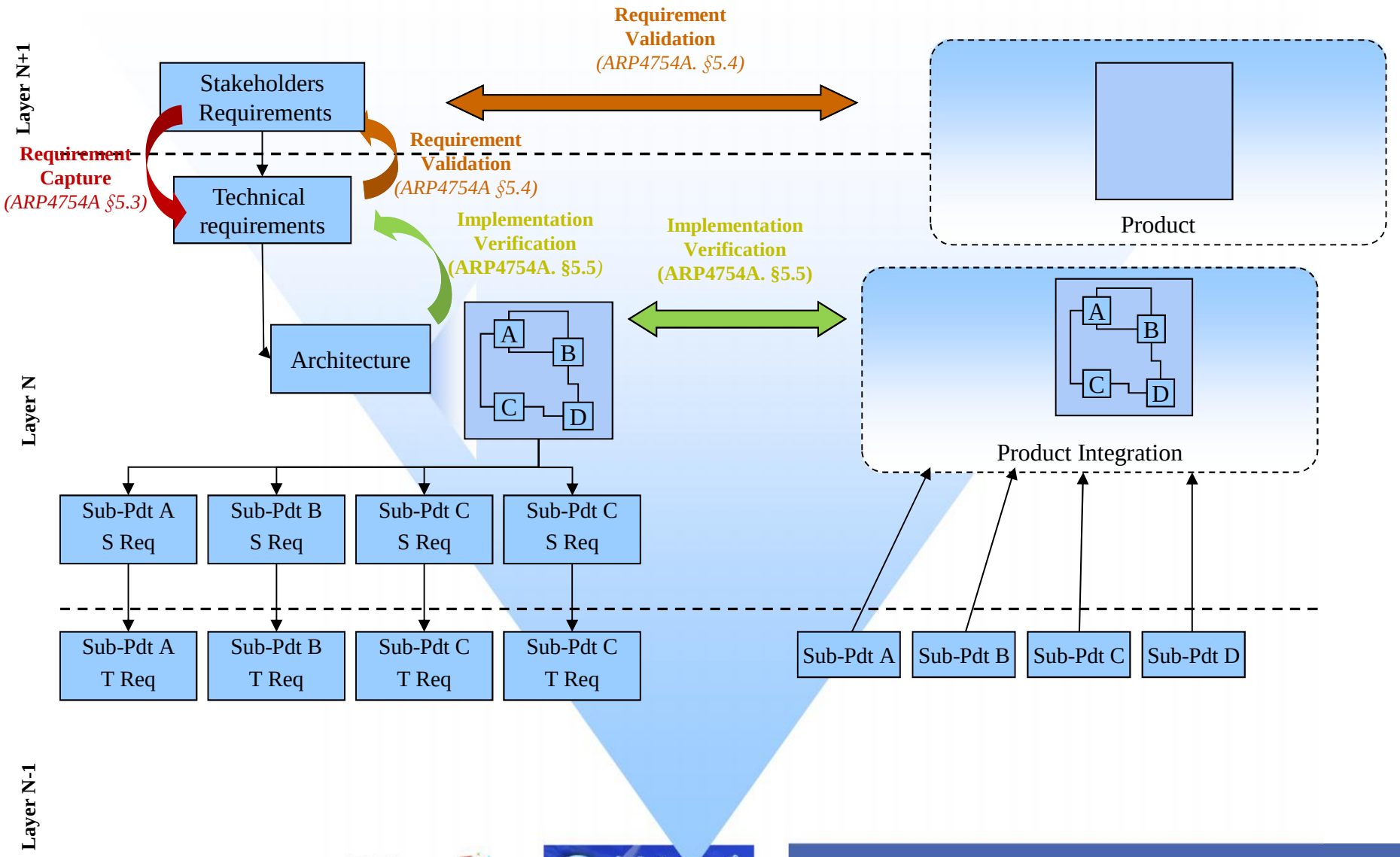
- Certification credits would be harder and more costly to obtain with other practices

ARP 4754A keywords

www.wordle.net

Focus on Requirements Management (RM) and Verification&Validation (V&V)

Certification-oriented engineering



The V&V required documents

According to the Development Assurance Level (DAL), some documents are mandatory for certification (extract from ARP 4754):

DAL / Documents	A - B	C	D	E
V&V plan	R	R	A	N
Validation matrix	R	R	A	N
Verification matrix	R	R	A	N
Requirements traceability	R	A	A	N
Verification procedures	R	A	A	N
Verification means (Inspection, review, analysis, test)	Test and at least one other	At least one	A	N
V&V Summary	R	R	A	N

R: Recommended (“mandatory”)
A: As negotiated
N: Not required for certification