CSD&M
October 27-29, 2010
Complex Systems Design & Management 2010

# Information model for model driven safety requirements management of complex systems

Romaric GUILLERM
Hamid DEMMOU
*LAAS-CNRS*

Nabil SADOU
*SUPELEC/IETR*

# Outline

- General context and motivation
- Design framework
- Information model
- Conclusion

# General context

- Systems more and more complex
  → Complex design processes
- Stronger constraints of safety (standards, certification authorities…)
- Hard competition (cost and time…)

➔ Weaknesses of the current safety processes

# General context

- Weaknesses of the current safety processes [Rasmussen 97]
  - Absence of a common language between the various trades involved with the system
  - Different groups need to work with different views of the system (e.g. systems engineers' view, safety engineer's view). This is a weakness if the views are not consistent.
  - Bad definition of the safety requirements and their formalization
  - Absence of traceability of safety requirements
  - Existing methods (traditional) are insufficient to deals with the complexity of the current systems

# Motivation

- Global approach for the safety consideration is needed
  - Taking into account the risks associated with the integration of the system
  - Taking into account the safety requirements throughout the all lifecycle of the system
- Efficient requirements management is needed
  - Formalization of the requirements
  - Traceability management
  - Use of a common language

# Propositions

- Global approach for safety
  - Well adapted framework: **System Engineering**
  - Objective: taking into account the safety early in the design, and in an overall study (system level)

- MDE (Model Driven Engineering) approach for a better consideration of safety requirements
  - **Information model**
  - Common language
  - Requirements formalization
  - Traceability and links with the rest of the design and the V&V activities

# Design framework

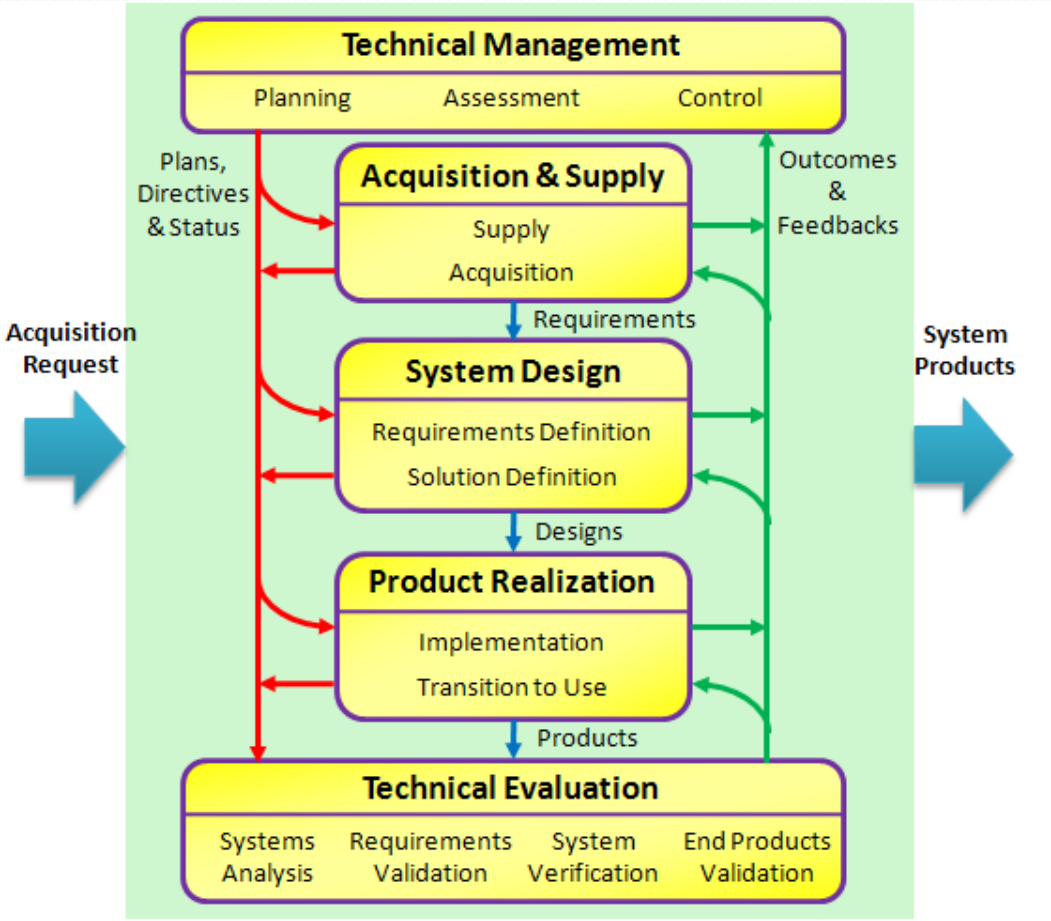
- System Engineering - Definition

> System Engineering is a general methodological approach that encompasses all activities appropriate to design, develop and test a system providing efficient and economical solution to client's needs while satisfying all stakeholders. [AFIS]

- A framework for the development of complex systems
- EIA-632 standard
- Methodological guide for the consideration of safety in the SE processes:
  - Processes of EIA-632 translated and refined in terms of safety

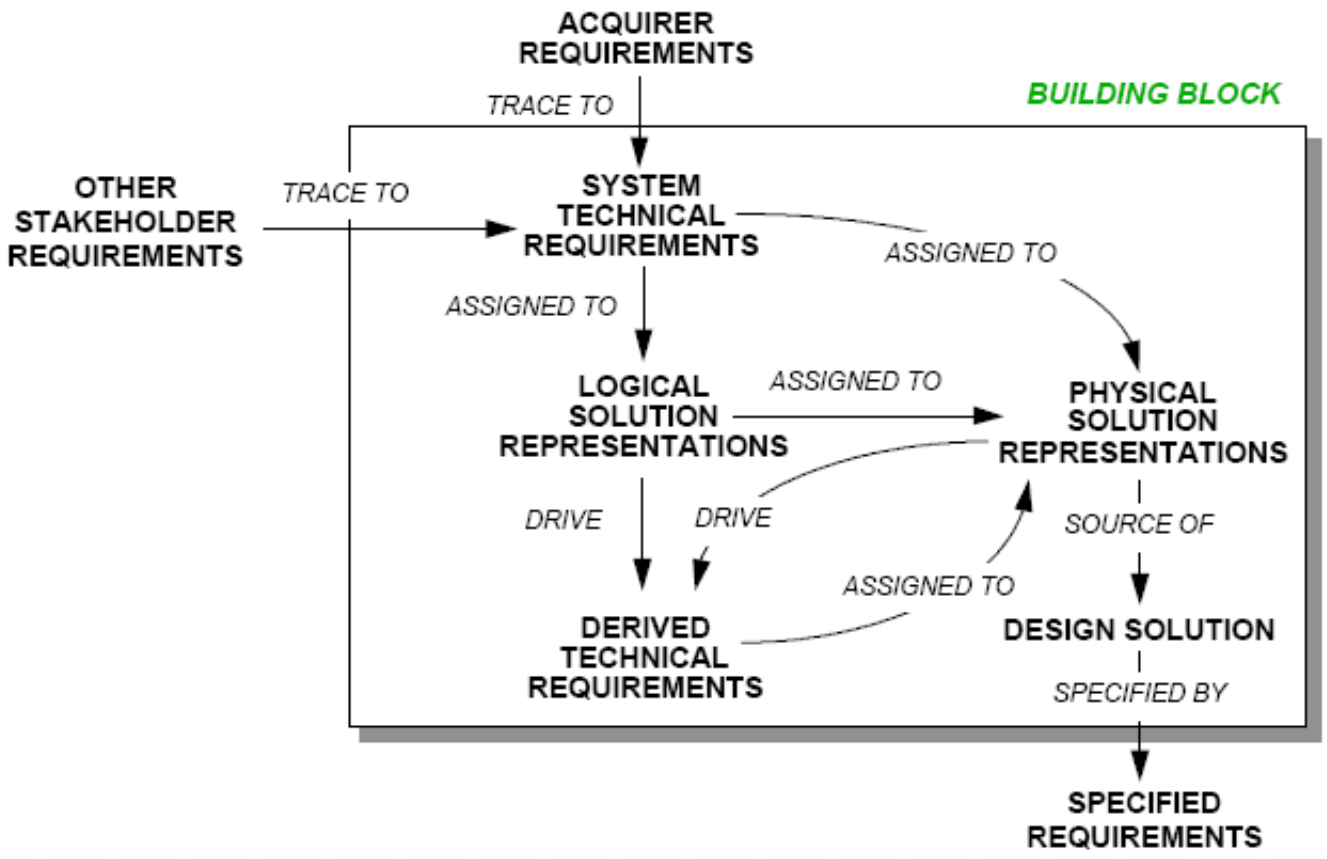
# Design framework

- EIA-632 standard – Processes



# Design framework

- EIA-632 standard – Requirements management



# Information model

**Why**?

- Make effective requirements management
- Manage requirements changes
- Help impact analysis
- Guide the design
- Evaluate project progress

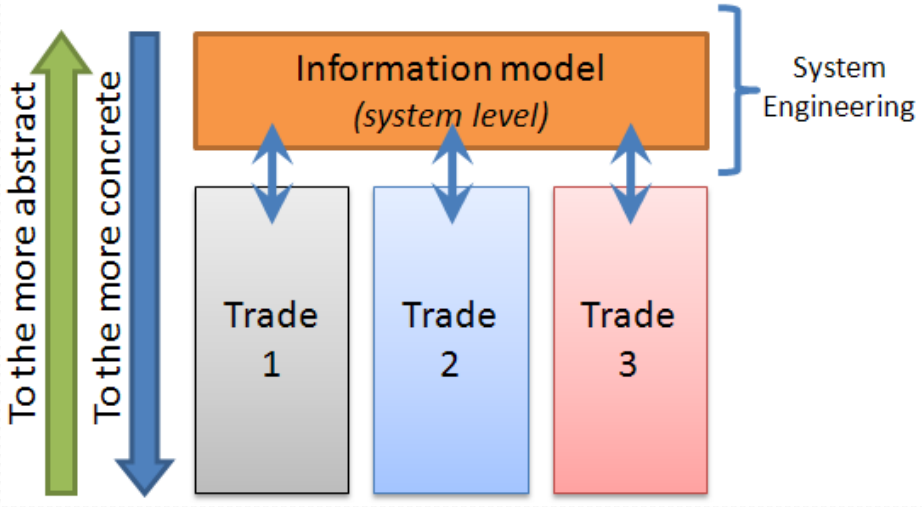
- Be the basis of knowledge of the design project, proposing a shared model with a common language understandable by different persons involved in the project

# Information model

- The information model is intended to model the « system » level
- Shares the knowledge between the different trades and specialties, including the 3 components:

  *Requirements - Design solution - V&V*

- The elements of V&V are included in the model to be directly linked to the requirements they satisfy.

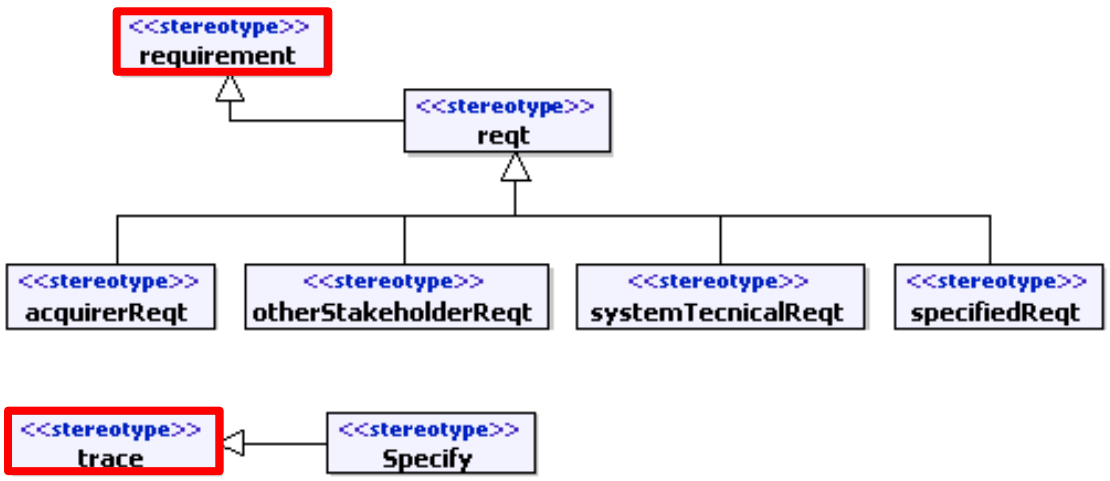


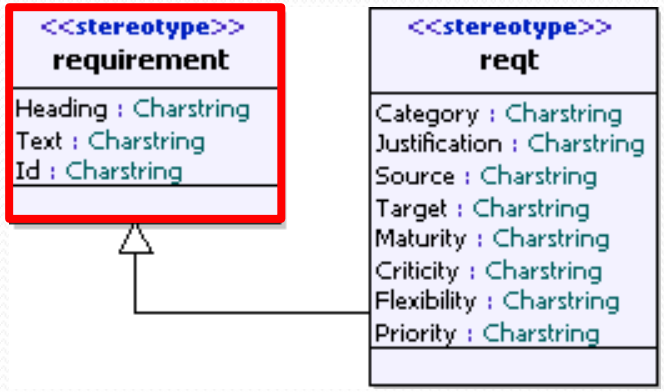
# Information model

- Chosen language: SysML
  - Common language
  - Allows modeling a wide range of systems
  - Good expression of requirements (with all relevant information)
  - Rigorous traceability: facilitates impact analysis (example: change of requirements)
  - Visible allocation of requirements on the model
  - Integration and  association of test cases directly to the model
  - SysML extensibility (adding information about the risks and expected safety properties)

# Information model

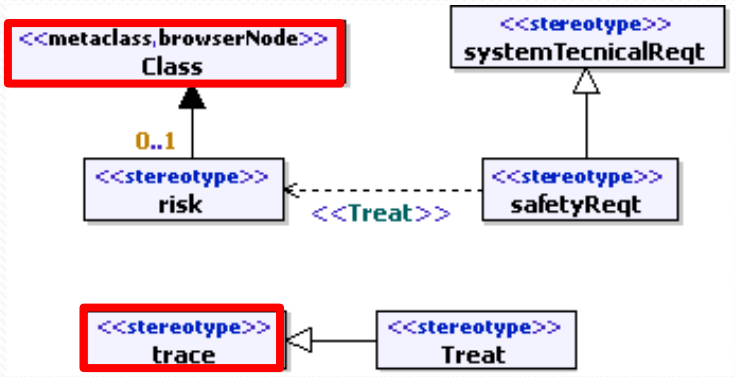
- We have extended SysML :
  - New stereotypes for the requirements
  - New attributes for the requirements
  - Definition of a new link (*specify*) to connect the specified requirements to model elements



# Information model

- We have extended SysML :
  - New block « *risk* » linked to safety requirements
  - Definition of a new link (*treat*) to connect the safety requirements to the risks that they deal

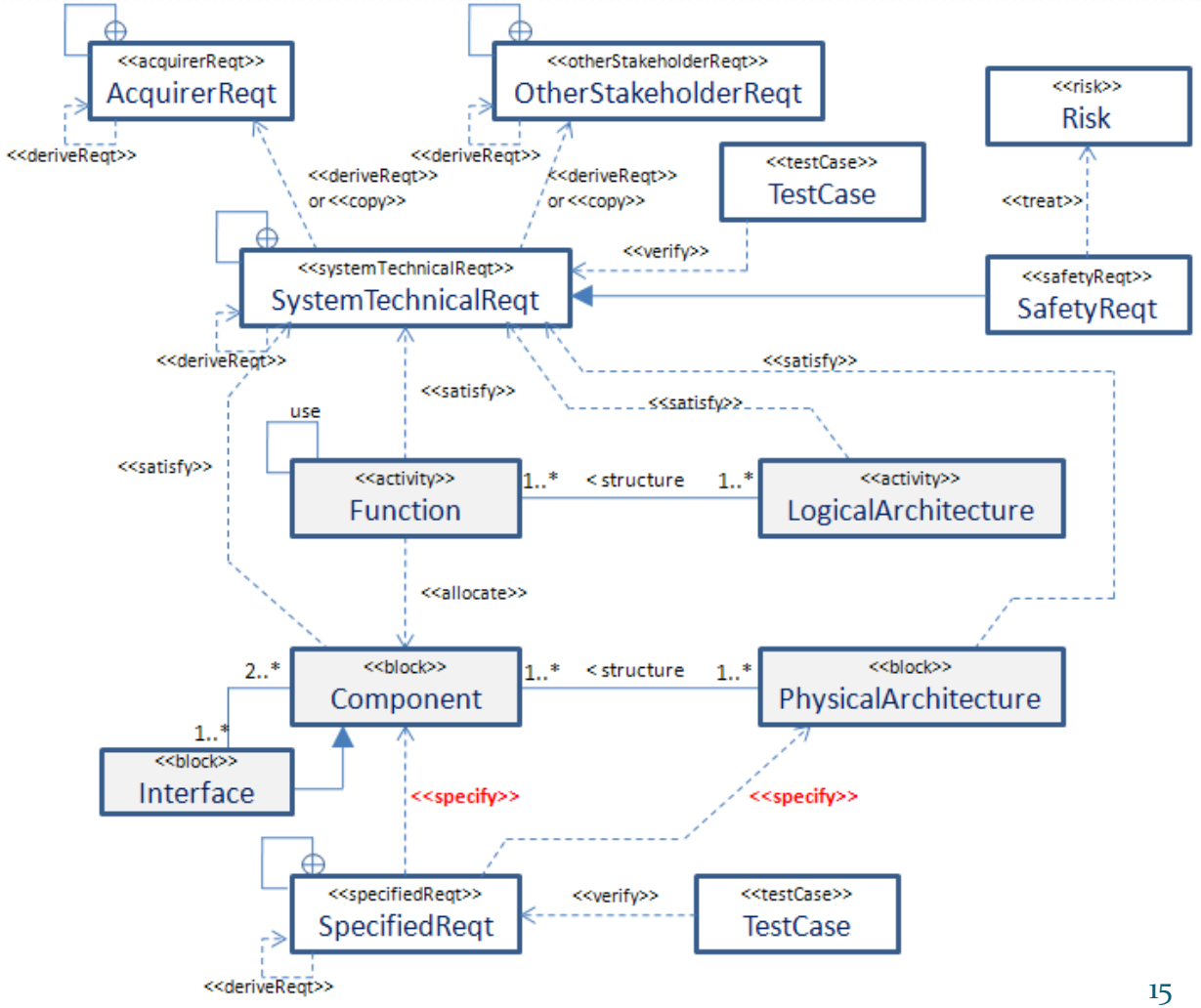



# Information model

**Information model**

=

**meta-model** for the design of safe system



# Conclusion

- As part of the overall approach of safety:
  - Definition of an information model
    - Using SysML, a common language, and some extensions
    - Adapted to the EIA-632 standard
    - Integrating safety concepts (safety requirements and risks)
    - Supporting the requirements management, with a rigorous traceability between elements
  - Work in progress: An example will validate the approach

→ S18 aircraft extracted from the ARP-4761 standard, with the consideration of the braking function and the components involved (reverses, spoilers, wheel brakes)

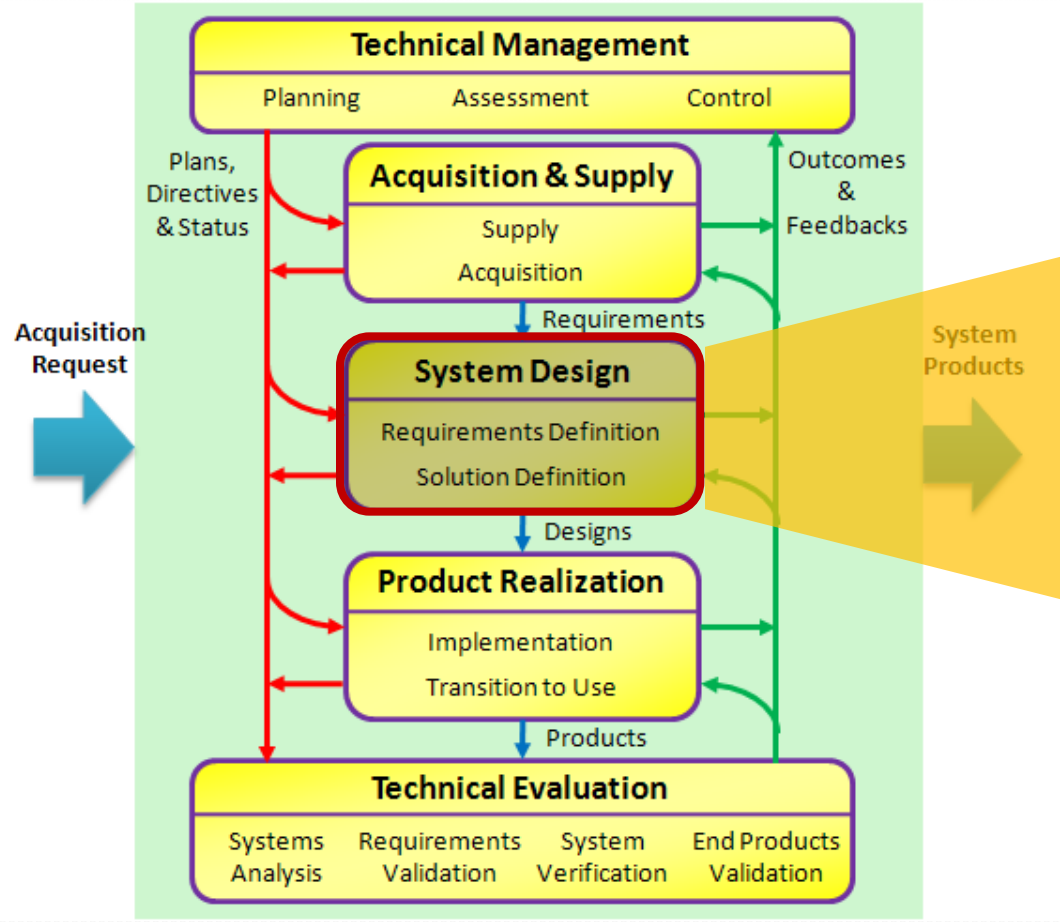
# Questions

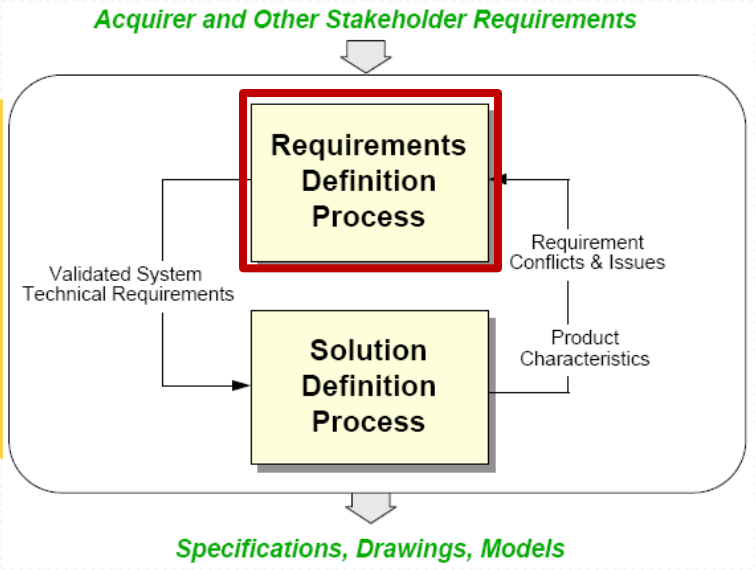
?

guillerm@laas.fr

# *Annexes*

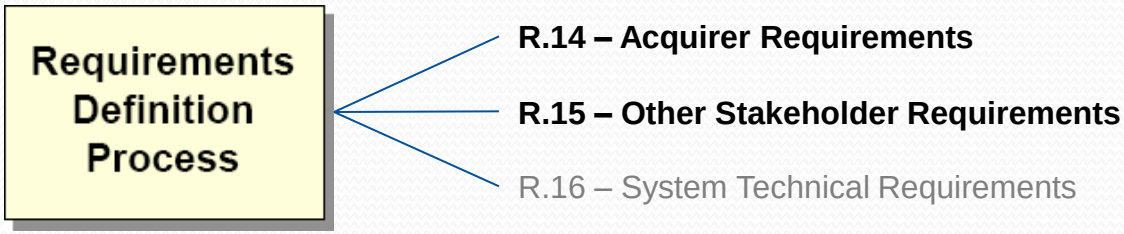
# Safety integration approach



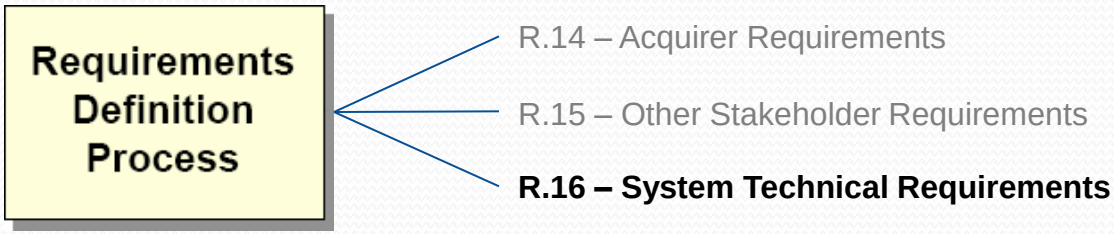

System Products

# Safety integration approach




- The developer shall define a validated set of acquirer (other stakeholder) requirements for the system, or portion thereof.
- In the safety framework:
  - Acquirer requirements, generally, correspond to constraints in the system. It is necessary to identify and collect all constraints imposed by acquirer to obtain a dependable system.
  - A hierarchical organization associates weight to safety requirements, following their criticality.
  - Safety requirements can be derived from certification or quality requirements or can be explicitly expressed by acquirer or other stakeholder.

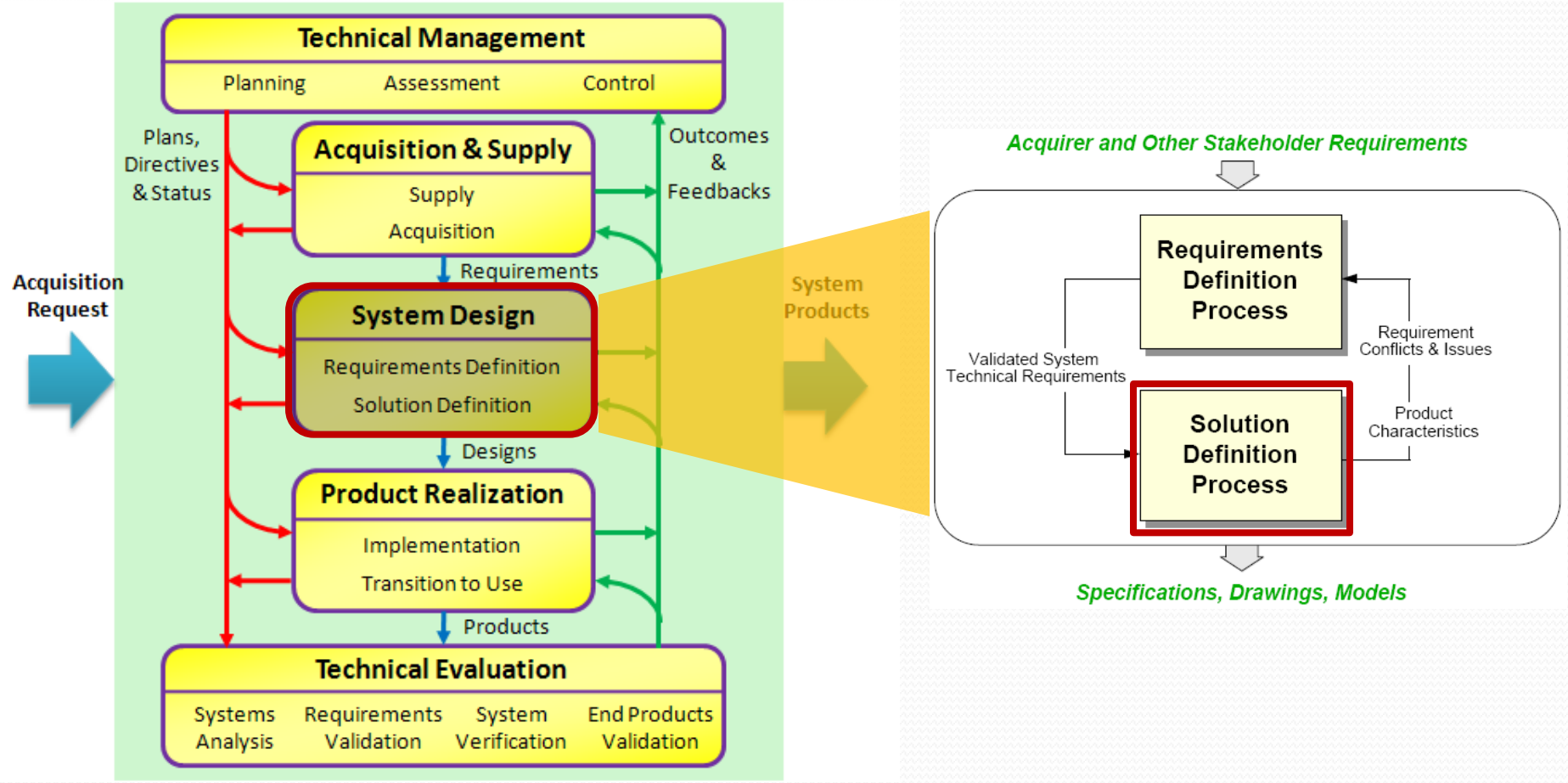
# Safety integration approach



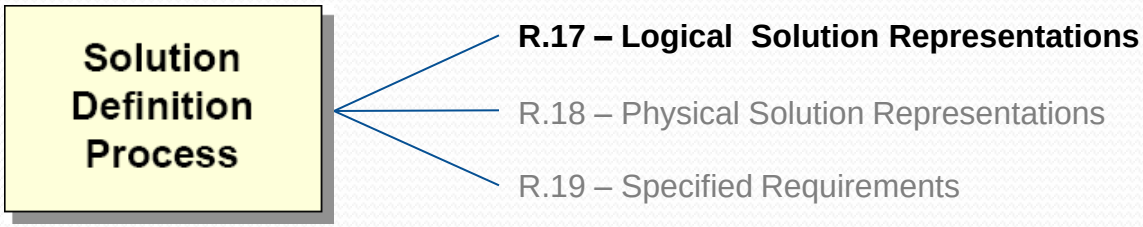

- The developer shall define a validated set of system technical requirements from the validated sets of acquirer requirements and other stakeholder requirements.
- Concerning safety:
  - System technical requirements traduce system performances
  - It consists on defining safety attributes (SIL level, MTBF(1), MTTR(2), failure rate,…)
  - Technical requirements can be derived from a preliminary hazard analysis.
  - Some standard can help designer to define safety requirements.
    Example in civil aerospace sector: ARP4754 and ARP 4761.

(1) Mean Time Between Failure, (2) Mean Time To Repair

# Safety integration approach

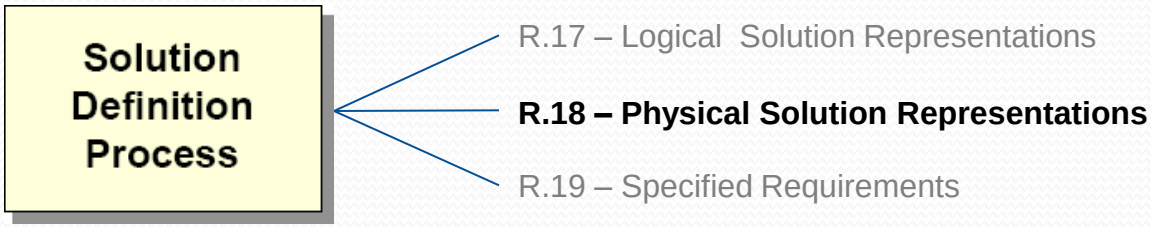


# Safety integration approach



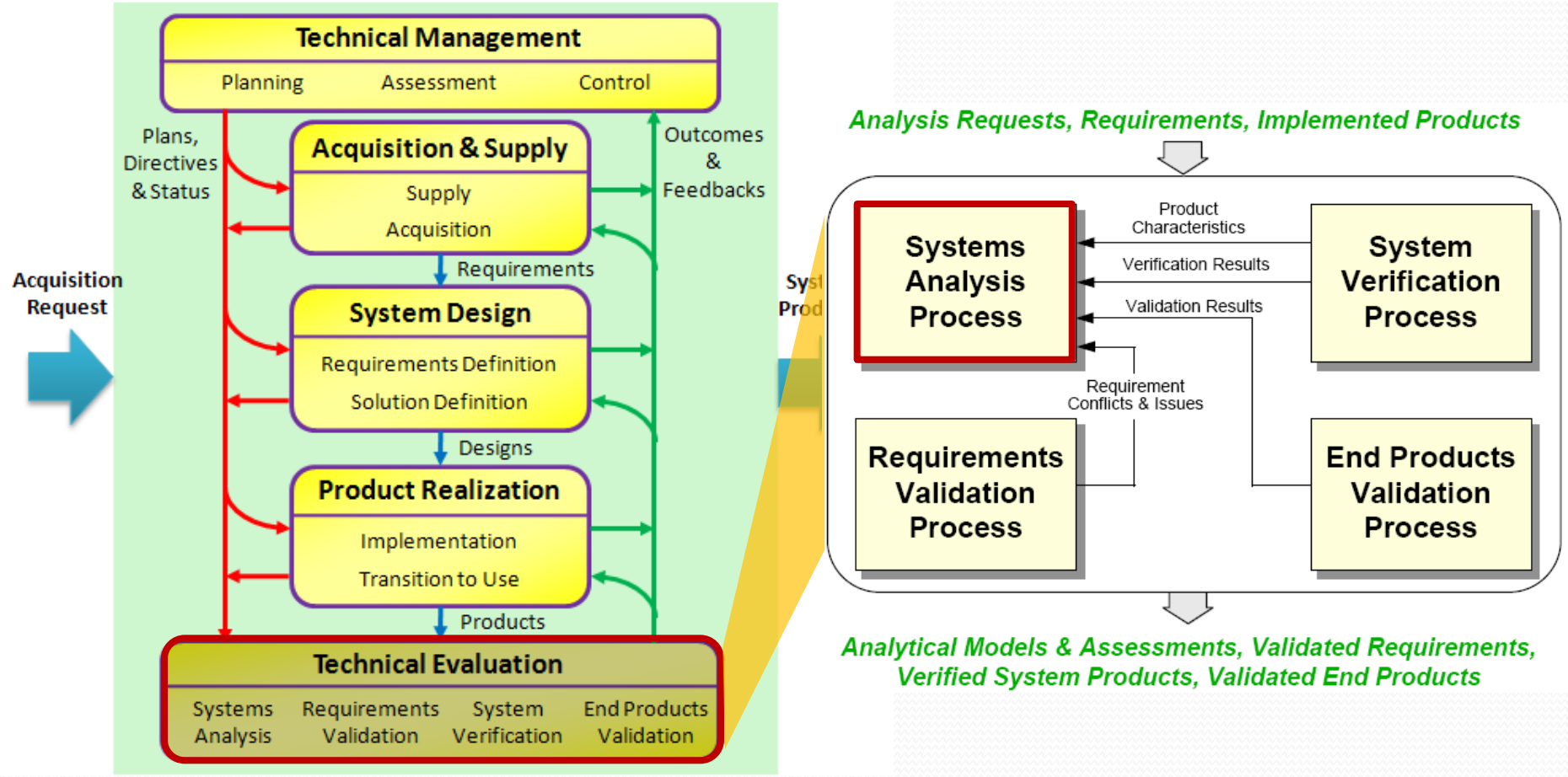

- The developer shall define one or more validated sets of logical solution representations that conform with the technical requirements of the system.
- The recommendation is to use semi formal / formal models for the solution modeling. The use of formal methods allows for automation of verification and analysis.
- In this processes, safety analysis techniques will be used to determine the best logical solution.

# Safety integration approach

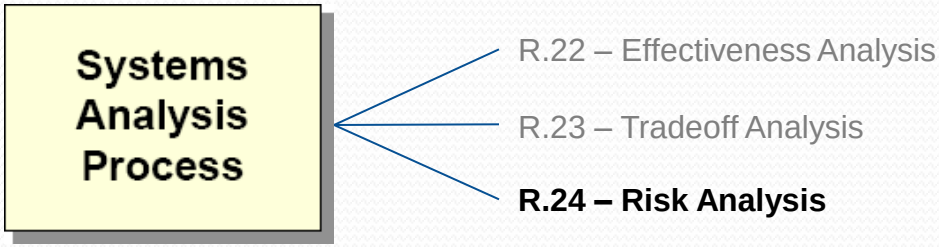



- The developer shall define a preferred set of physical solution representations that agrees with the assigned logical solution representations, derived technical requirements, and system technical requirements.
- The physical solution representations are derived from logical solution representation and must respects all requirements, particularly safety requirements.
- The same safety analysis may be done for the physical solution representations. The same recommendations than for logical solution remain true.

# Safety integration approach



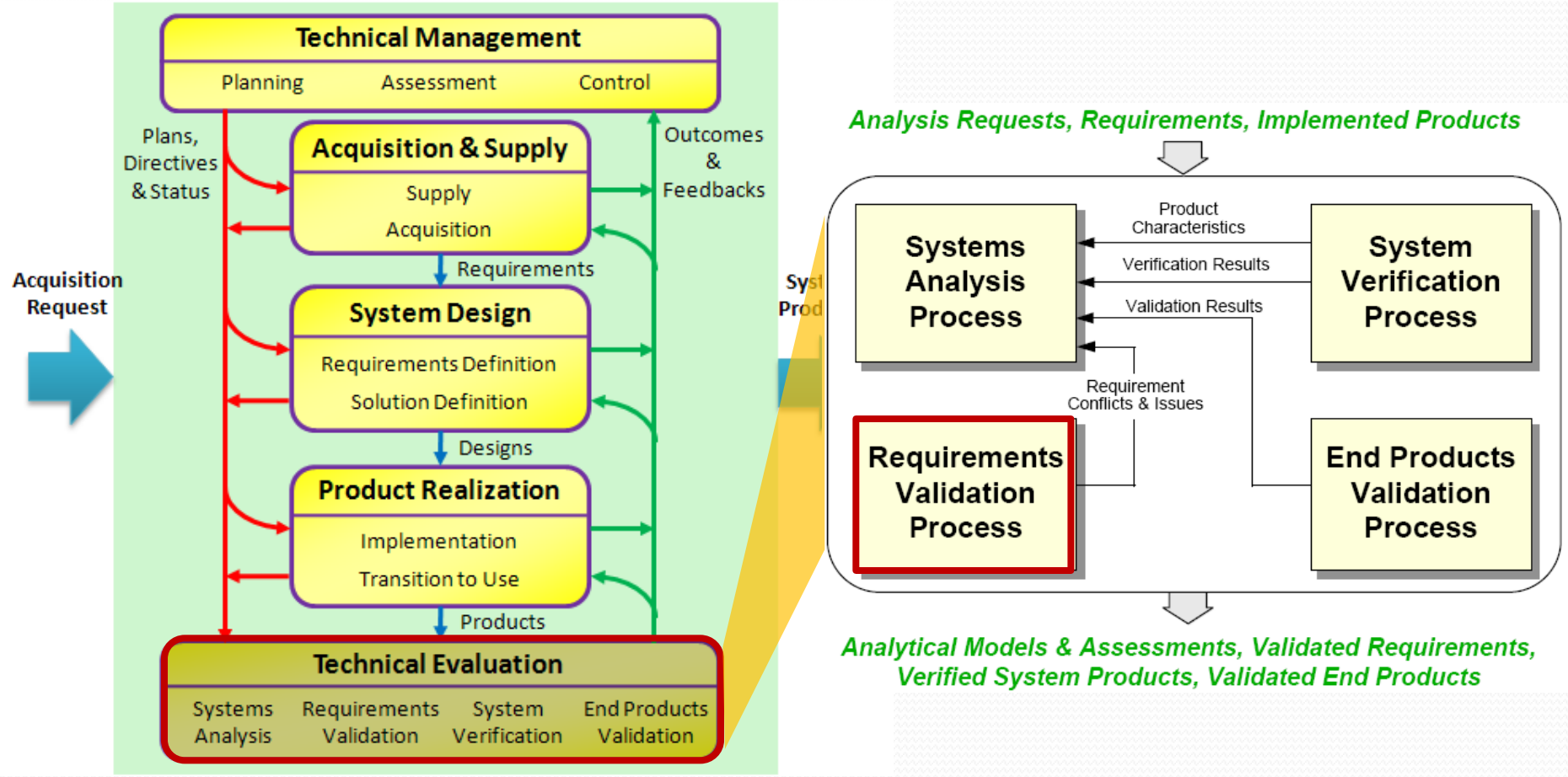
# Safety integration approach



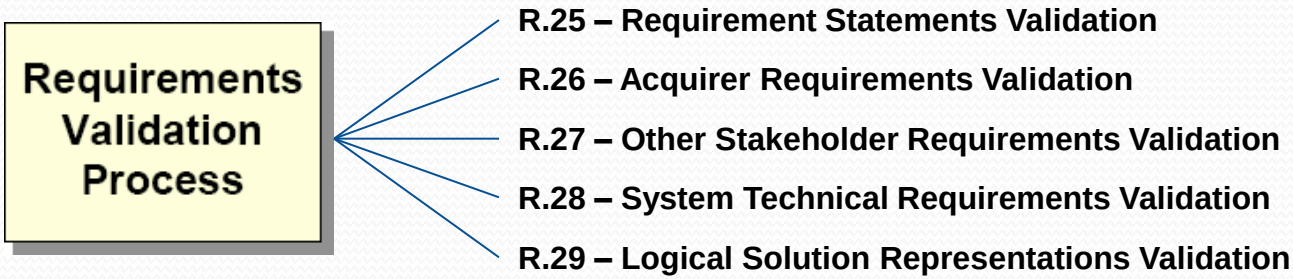

- The developer shall perform risk analyses to develop risk management strategies, support management of risks, and support decision making.

- Techniques: Fault tree ; Failure Mode, Effect, and Criticality Analysis; …
- Determines the risks of the system
- Can generate safety requirements other than that defined by the acquirer and other stakeholders.

# Safety integration approach

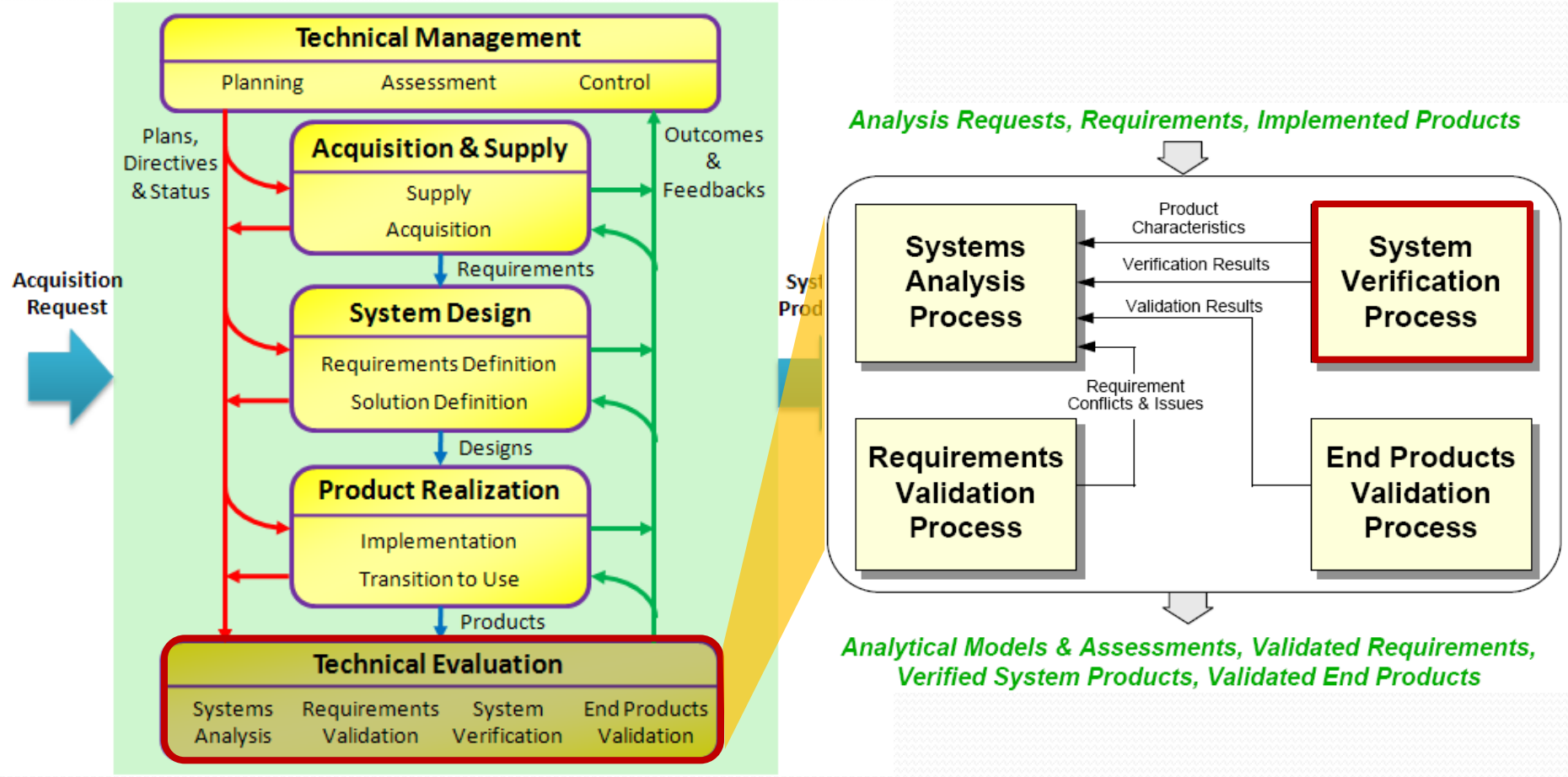


# Safety integration approach

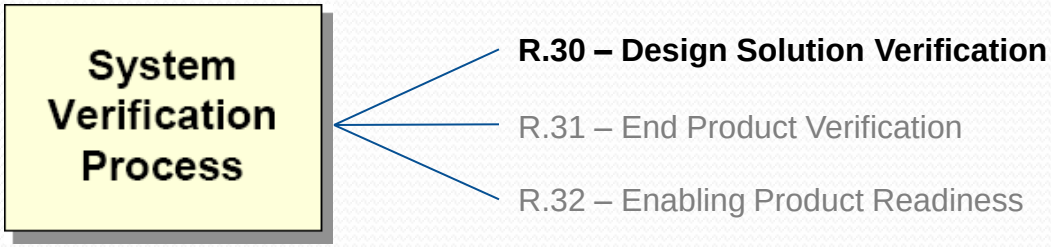



- Requirements Validation is critical to successful system product.
- Requirements are validated when it is certain that they describe the input requirements and objectives such that the resulting system products can satisfy them.
- A great attention is done to traceability analysis.
- Like other requirements, safety requirements must be validated. The validation allows designing safe system.
- To facilitate this step, semi-formal solutions, like UML or SysML, can be used for good formulation of requirements.

# Safety integration approach



# Safety integration approach




- The System Verification Process is used to ascertain that:
  - The generated system design solution is consistent with its source requirements, in particular safety requirements.
- Some traceability models allow defining the procedure of verifying safety requirement. These procedures are planned at the definition of safety requirement.
- Simulation is a good and current method used to achieve system verification
- Other methods: virtual prototyping, model checking,…