Systems Engineering and Project Management (Introduction)

Prof. Dr. Franz Wotawa

Institute of Software Engineering and Artificial Intelligence

wotawa@tugraz.at

What is Systems Engineering?

What are Systems?

What are Systems?

- *“A system is a set of interacting or interdependent component parts forming a complex/intricate whole.”*

- “*A system is an integrated composite of people, products, and processes that provide a capability to satisfy a stated need or objective.*”

What are Systems?

- IEEE Std 1220-1998: "*A set or arrangement of elements and processes that are related and whose behavior satisfies customer/operational needs and provides for life cycle sustainment of the products.*"
- ISO/IEC 15288:2008: "*A combination of interacting elements organized to achieve one or more stated purposes.*"

What are Systems?

- Systems have
  - Physical and temporal boundaries
  - An environment, interacting with the system
- Systens were described using
  - Their structure
  - Their purpose
  - Their functionality

What are Systems?

- Systems have a common characteristic:
  - Structure (components and their interconnections)
  - Behavior
  - Interconnectivity
- Systems can comprise other systems (which are called sub-systems)

What is engineering?

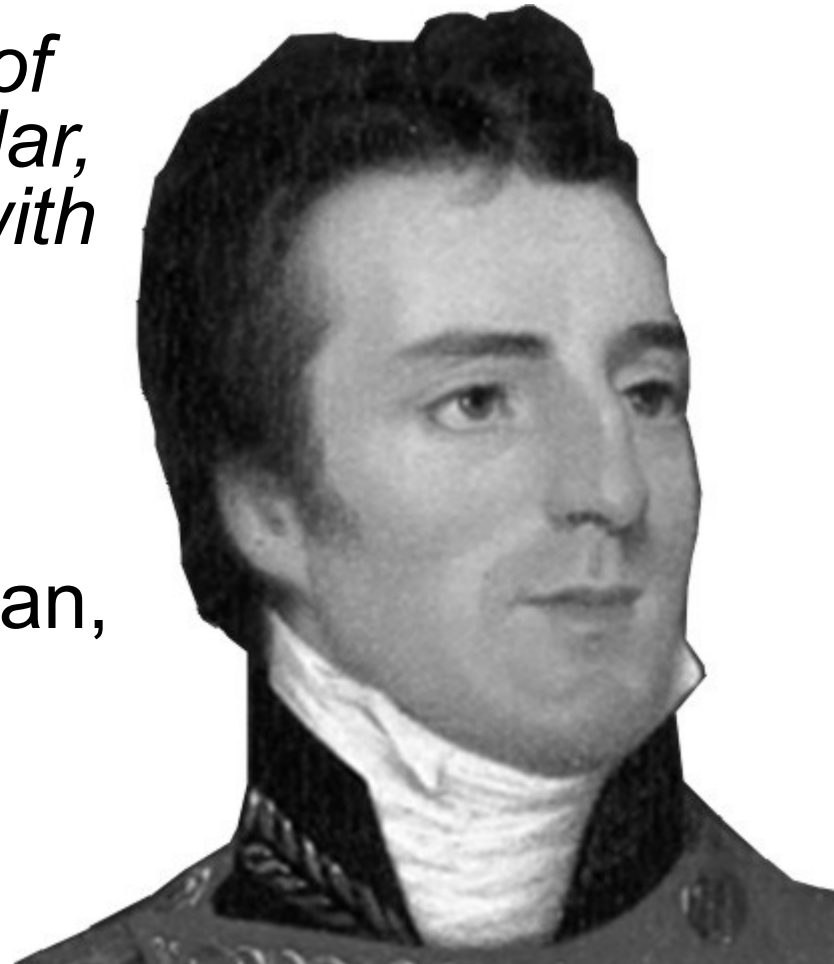
- *„Engineering is the application of mathematics, empiricism, and scientific, economic, social, and practical knowledge to invent, develop, manufacture, and maintain as well as improve structures, machines, tools, systems, components, materials, and processes.*

A Quote on Engineering

"To define it rudely but not ineptly,

ENGINEERING is the art of doing that well with one dollar, which any bungler can do with two after a fashion."

Duke of Wellington
Arthur Wellesley
1769-1852, British Statesman,
Military Leader



What happens in the case of bad engineering?

What is system engineering?

- System Engineering is a branch of engineering that focuses on the design and management of complex systems throughout their lifecycles.

What is system engineering?

- *"A logical **sequence** of **activities** and **decisions** that **transforms** an operational **need into** a description of system performance **parameters** and a preferred system **configuration**."*
  (MIL-STD-499A, Engineering Management, 1 May 1974.Now cancelled.)

- *"An interdisciplinary **approach** that encompasses the entire technical effort, and evolves into and verifies an integrated and life cycle balance set of **system people, products, and process solutions that satisfy customer need**s."*
  (EIA Standard IS-632, Systems Engineering, December 1994.)

- *"An interdisciplinary, collaborative **approach** that **derives, evolves, and verifies** a life-cycle balanced **system** solution which **satisfies customer expectations** and meets **public acceptability**."*
  (IEEE P1220, Standard for Application and Management of the Systems Engineering Process, [Final Draft], 26 September 1994.)

What is system engineering?

- Related disciplines:
  - Requirements Engineering
  - Reliability Engineering
  - Logistics
  - Control Engineering
  - Software Engineering
  - Project Management
  - …

What is system engineering?

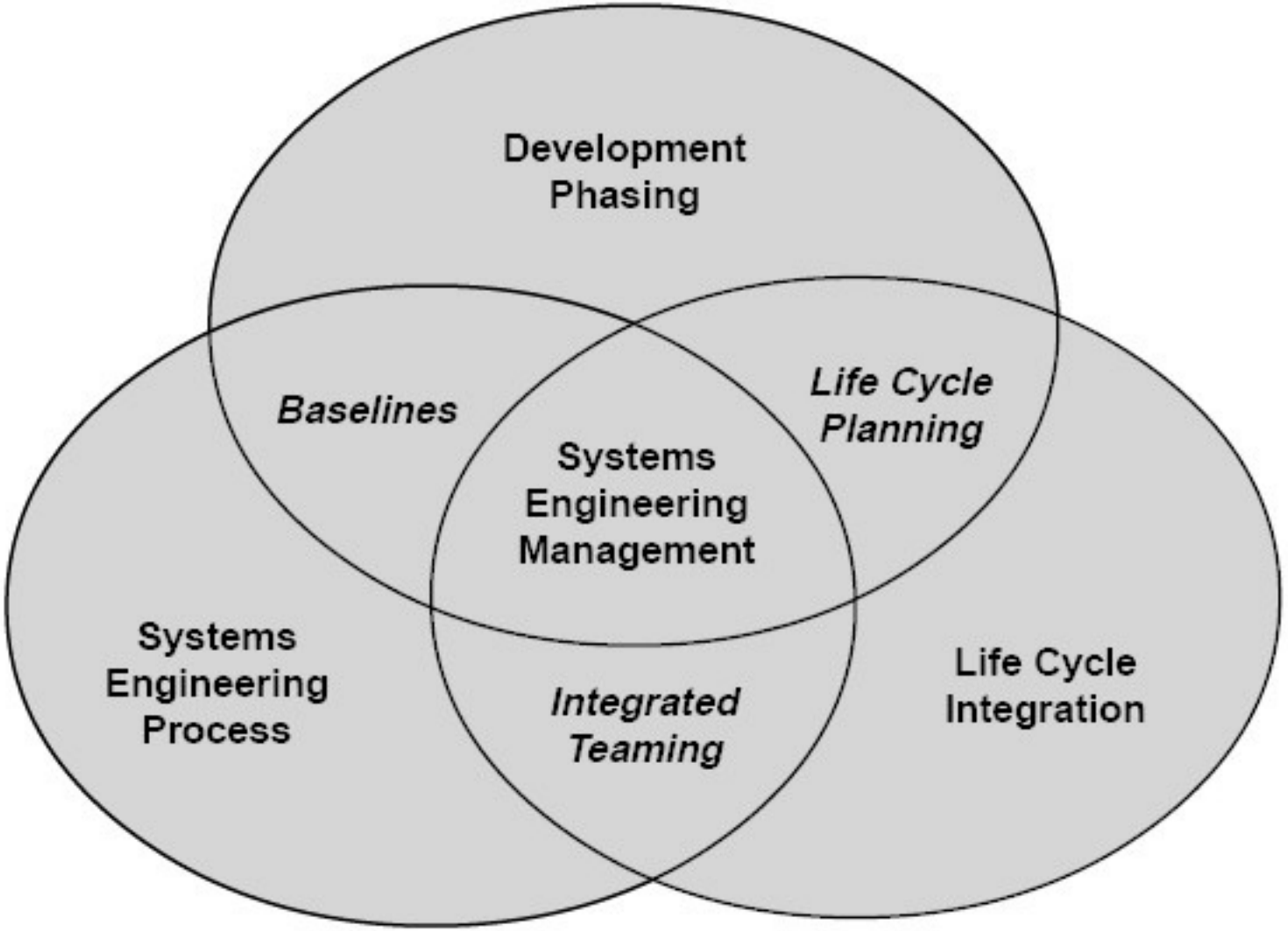
- What is the reason behind system engineering:

Managing Complexity!

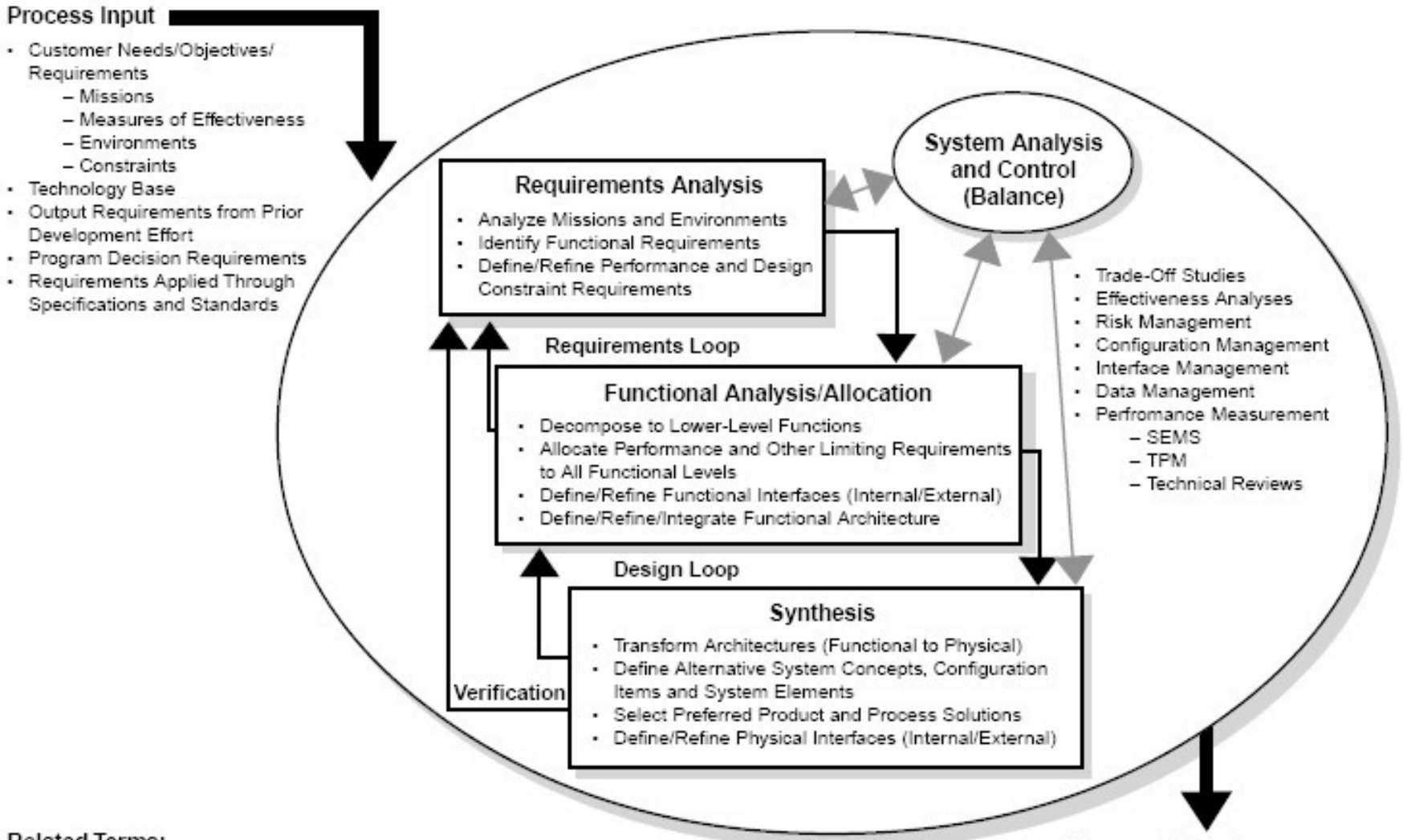
What is system engineering?

- Tools and methods:
  - System architecture,
  - System model, Modeling, and Simulation,
  - Optimization,
  - System dynamics,
  - Systems analysis,
  - Statistical analysis,
  - Reliability analysis, and
  - Decision making

Tasks of system engineering (SE)



SE process



Related Terms:

Customer = Organizations responsible for Primary Functions

Primary Functions = Development, Production/Construction, Verification, Deployment, Operations, Support, Training, Disposal

Systems Elements = Hardware, Software, Personnel, Facilities, Data, Material, Services, Techniques

Important tasks in SE

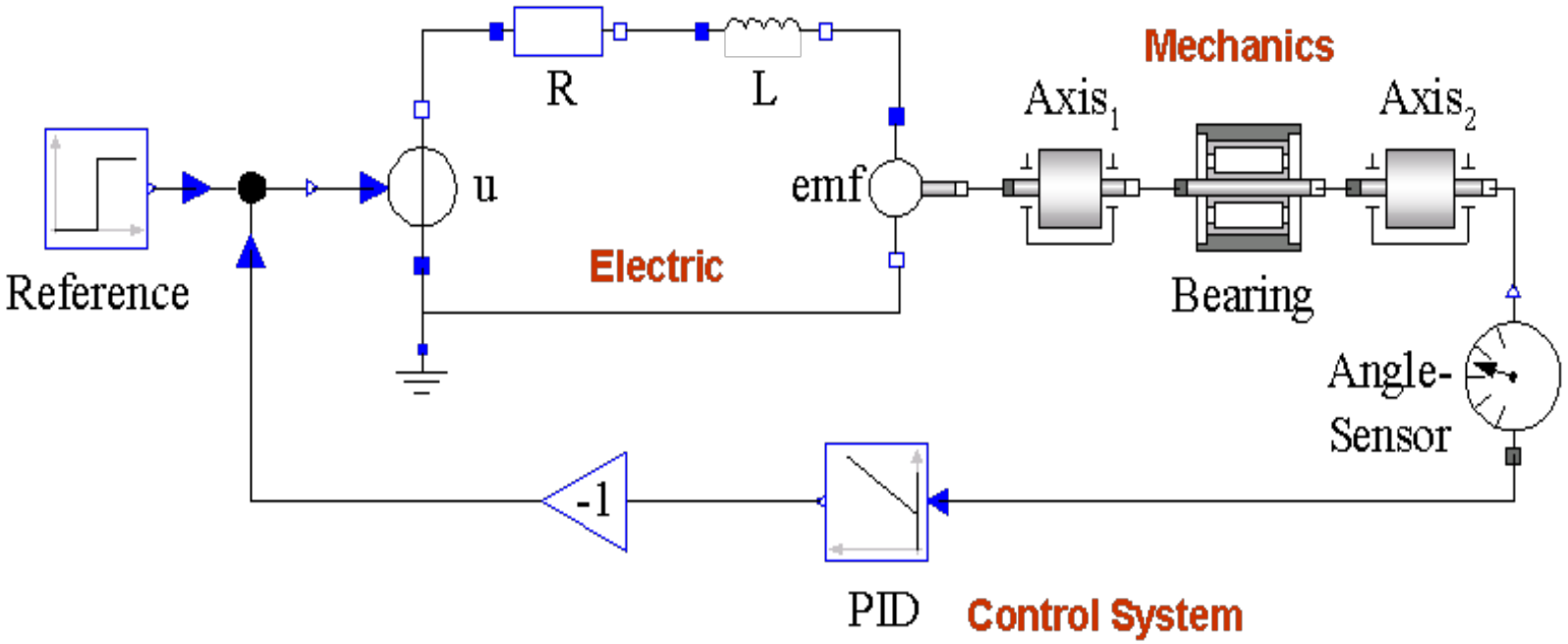
- Use of models and simulation to evaluate and validate the system's assumption
- Use of methods for the early prediction of faults and their consequences!

Safety Engineering

- To evaluate and take critical decisions as early as possible, considering their consequences.

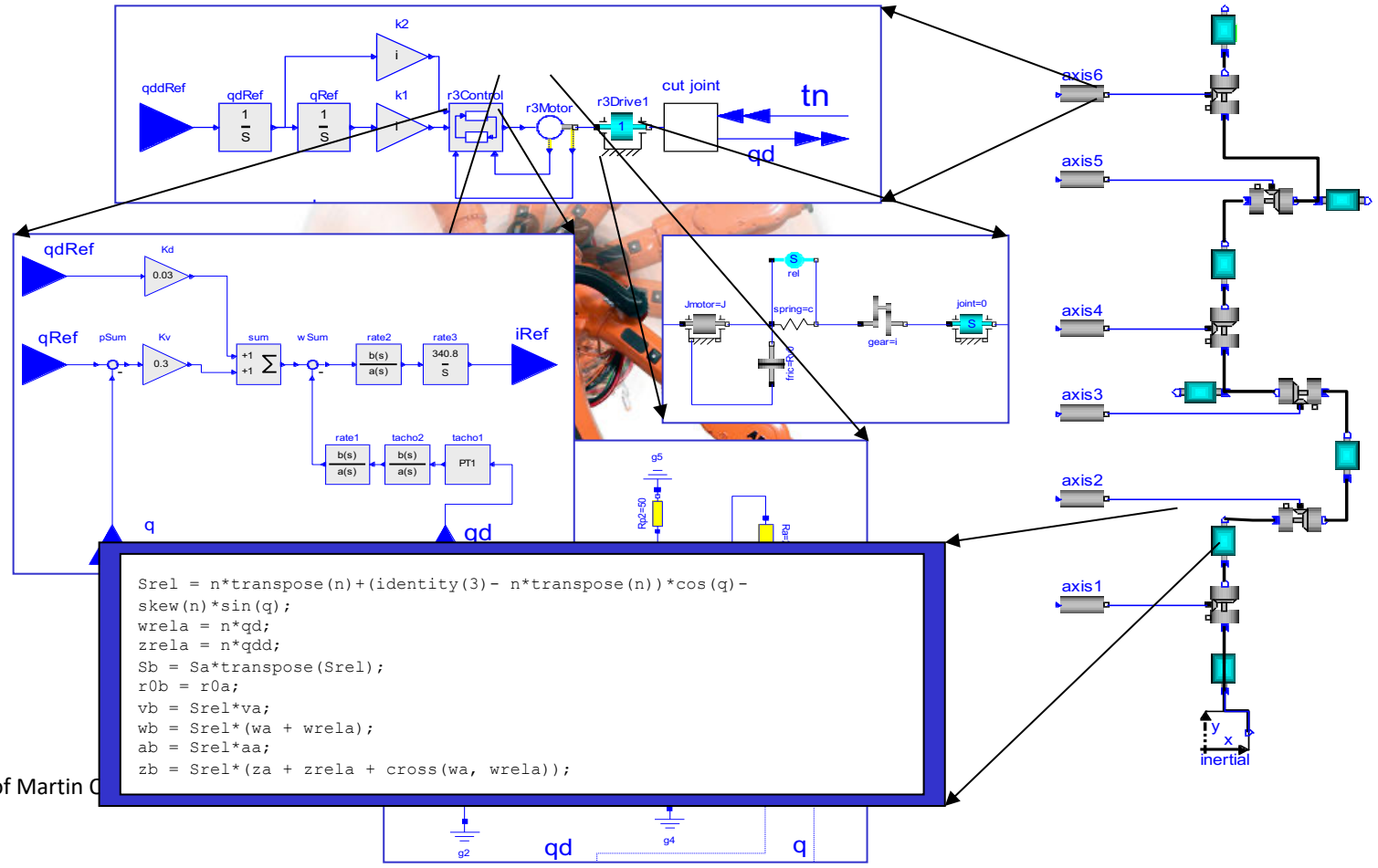
Simulation models

- Multi-domain models



Simulation models

- Hierarchical models



Courtesy of Martin C

Safety Engineering

- **Goal**: To make systems safe as demanded.
- Often based on risks.
- The risk r of a specific loss (or event) e is usually defined as a function of the probability p of the loss occurring and the costs c incurred if the loss occurs:

$$r(e) = p(e) * c(e)$$

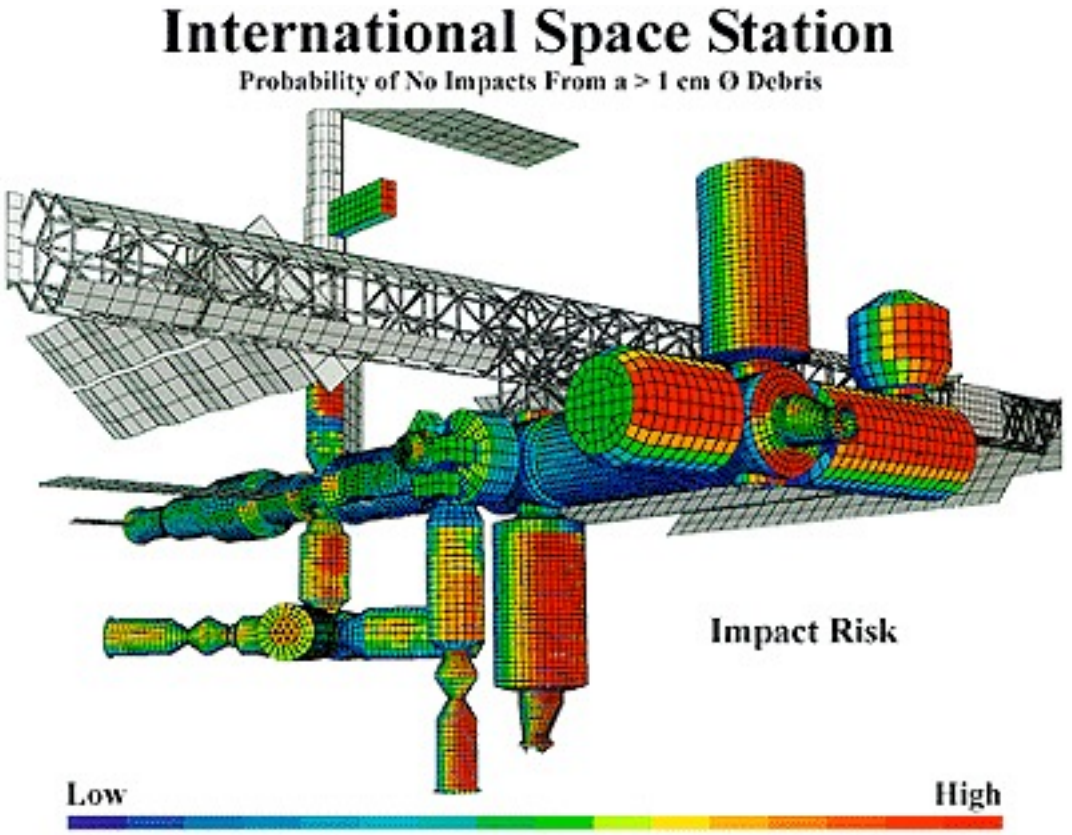
Safety Engineering

- Objective during development: Eliminate risks, or at least reduce them to a given and pre-defined boundary value.
-
- In most cases, it is not a quantitative statement that is important for risk, but a qualitative one!
  - Example: If human lives are at risk and an event is possible, then this event has a high risk, e.g.: ASIL D.

Safety Engineering

- Example: Risk distribution with regard to an impact at the International Space Station

Source: NASA



Techniques for risk estimation

- **Failure Mode and Effect Analysis (FMEA)**
  - Bottom up approach
  - Failure modes are identified for each system component.
  - For each failure mode, its effects are analyzed and assessed in terms of risk.

Techniques for risk estimation

- Example FMEA:

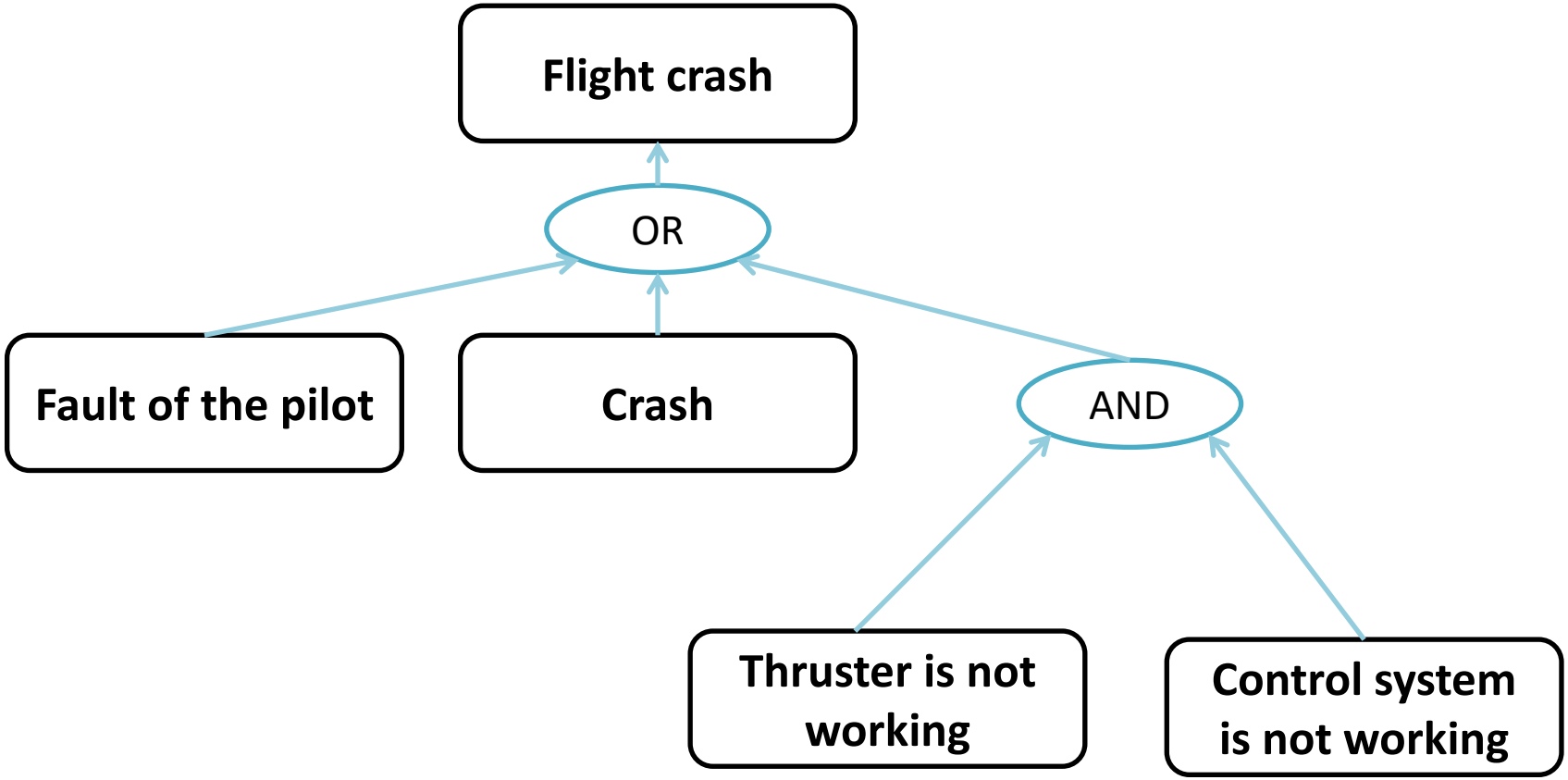
Component	Mode	Effect	risk
Tank system	To much fuel displayed	Cannot reach the goal	Average to high
Thruster	Not working	Causes differences on how to fly and redundancy	Average
Thruster	On fire	Causes differences on how to fly and redundancy	Average

Techniques for risk estimation

- Fault Tree Analysis (FTA)
  - Top down approach
  - Definition of top events such as a plane crash or a brake failure
  - Assignment of primary events component failure, human error, or external events to the top event using Boolean logic.

Techniques for risk estimation

- Example FTA:



What happens if the system has not been developed well (enough)?


Coca-Cola Media Player
Coca-Cola Media Player has encountered a problem and needs to close. We are sorry for the inconvenience.
If you were in the middle of something, the information you were working on might be lost.
Please tell Microsoft about this problem.
We have created an error report that you can send to us. We will treat this report as confidential and anonymous.
To see what data this error report contains, click here.
Send Error Report
Don't Send


Windows
An exception 06 has occured at 0028:C11B3ADC in VxD DiskTSD(03) +
00001660. This was called from 0028:C11B40C8 in VxD voltrack(04) +
00000000. It may be possible to continue normally.
* Press any key to attempt to continue.
* Press CTRL+ALT+RESET to restart your computer. You will
lose any unsaved information in all applications.
Press any key to continue

How Vulnerable Is Your Car to Cyber Attack?

As cars barrel toward full electronic control, are they vulnerable to cyber attack?

By Glenn Derene

0 +1 Share Like 2 Send it Tweet

Displaying an arbitrary message and a false speedometer reading on the Driver Information Center. Note that the car is in Park.

June 21, 2010 1:00 PM

TEXT SIZE: A . A . A

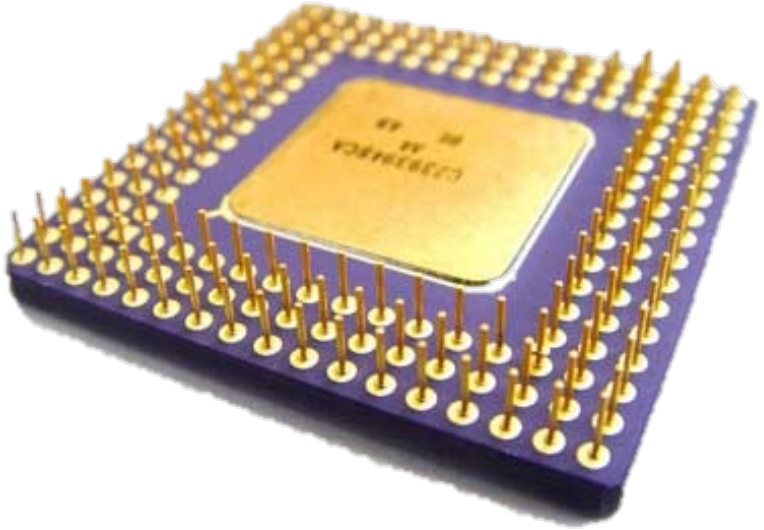
Last November, on a closed airport runway north of Seattle, Wash., a team of researchers from University of Washington and University of California–San Diego performed an ominous experiment on a late-model sedan. With a chase car driving on a parallel runway, they sped the test vehicle up to 40 mph, then turned off the brakes—via Wi-Fi. "Even though we knew what was going to happen, it's a very unsettling feeling to have a loss of control," says Alexei Czeskis, the researcher who was driving the test car. "You get full resistance from the brake pedal, but no matter how hard you press, nothing happens."

The test sedan was rigged up with a laptop hooked into its OBD II diagnostic port. On the computer was a custom-coded application, called CarShark, that analyzes and rewrites automobile software. That laptop was linked via a wireless connection to another laptop in the chase car. In addition to temporarily rendering the test car brakeless, the setup also allowed the research team to remotely turn off all the vehicle's lights (including the headlights and brake lights), turn on the windshield wipers, honk the horn, pop the

SPECIAL OFFER
GET Popular Mechanics
EVERY MONTH

Popular Mechanics, 2010

- **3-5 million ICs were affected by an error in the division of numbers**
- **$ 475 million costs of this damage**



Quelle: http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=2

- **Error in converting a number to another number system**
- **Excessive thrust caused the explosion**
- **$370 million in damage**

Quelle: http://www.wired.com/software/coolapps/news/2005/11/69355?currentPage=2

Zündschloss-Probleme bei GM: Die Tragödien hinter dem Rückruf

Opel

Opel GT: Auch 1200 Modelle in Deutschland sind vom Rückruf betroffen

Kleiner Fehler, tödliche Wirkung: Durch Zündschloss-Probleme bei GM-Modellen sollen mindestens zwölf Menschen ums Leben gekommen sein. US-Verbraucherschützer hingegen gehen von deutlich höheren Opferzahlen aus. Auch in Deutschland sind 1200 Opel-Modelle vom Rückruf betroffen.

Teilen Empfehlen 88 Twittern 27 G+1

Freitag, 14.03.2014 – 17:49 Uhr

From www.spiegel.de

SE Grundlagen & Ansatz

- Nach dem NASA/SP-2007-6105 Rev1 Systems Engineering Handbook

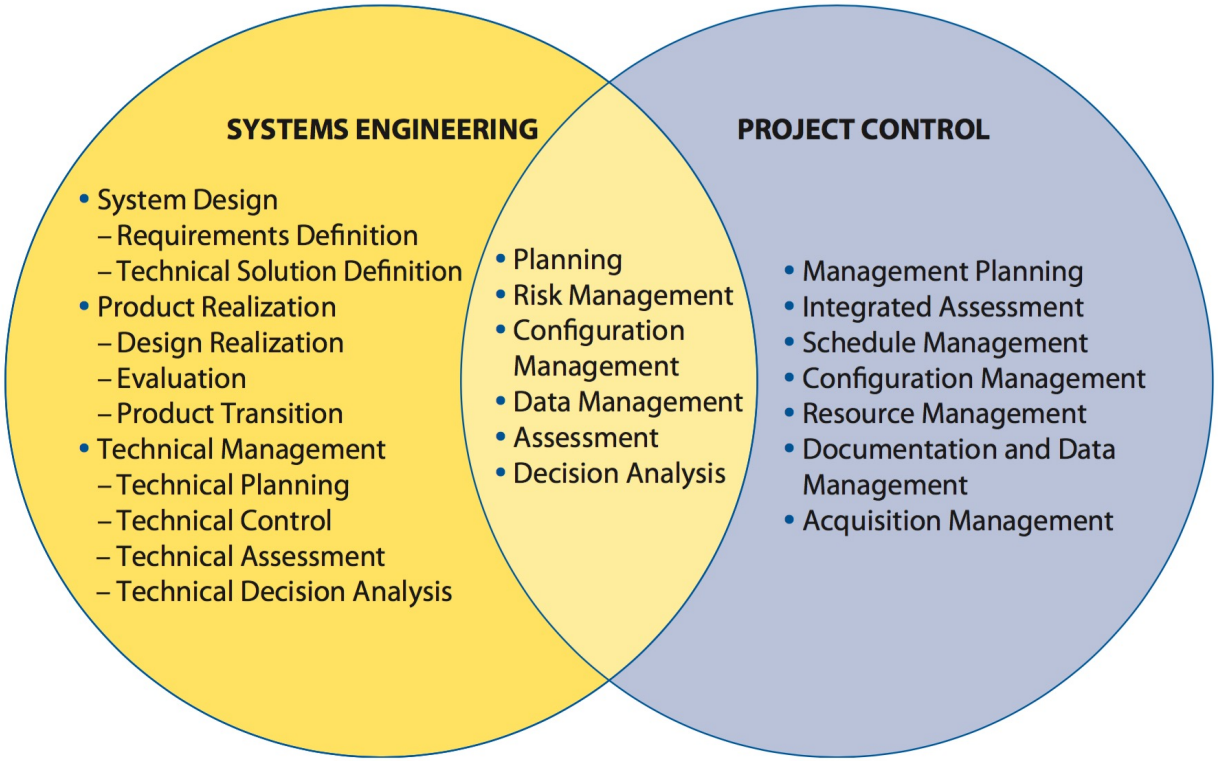


Figure 2.0-1 SE in context of overall project management

SE Design Process

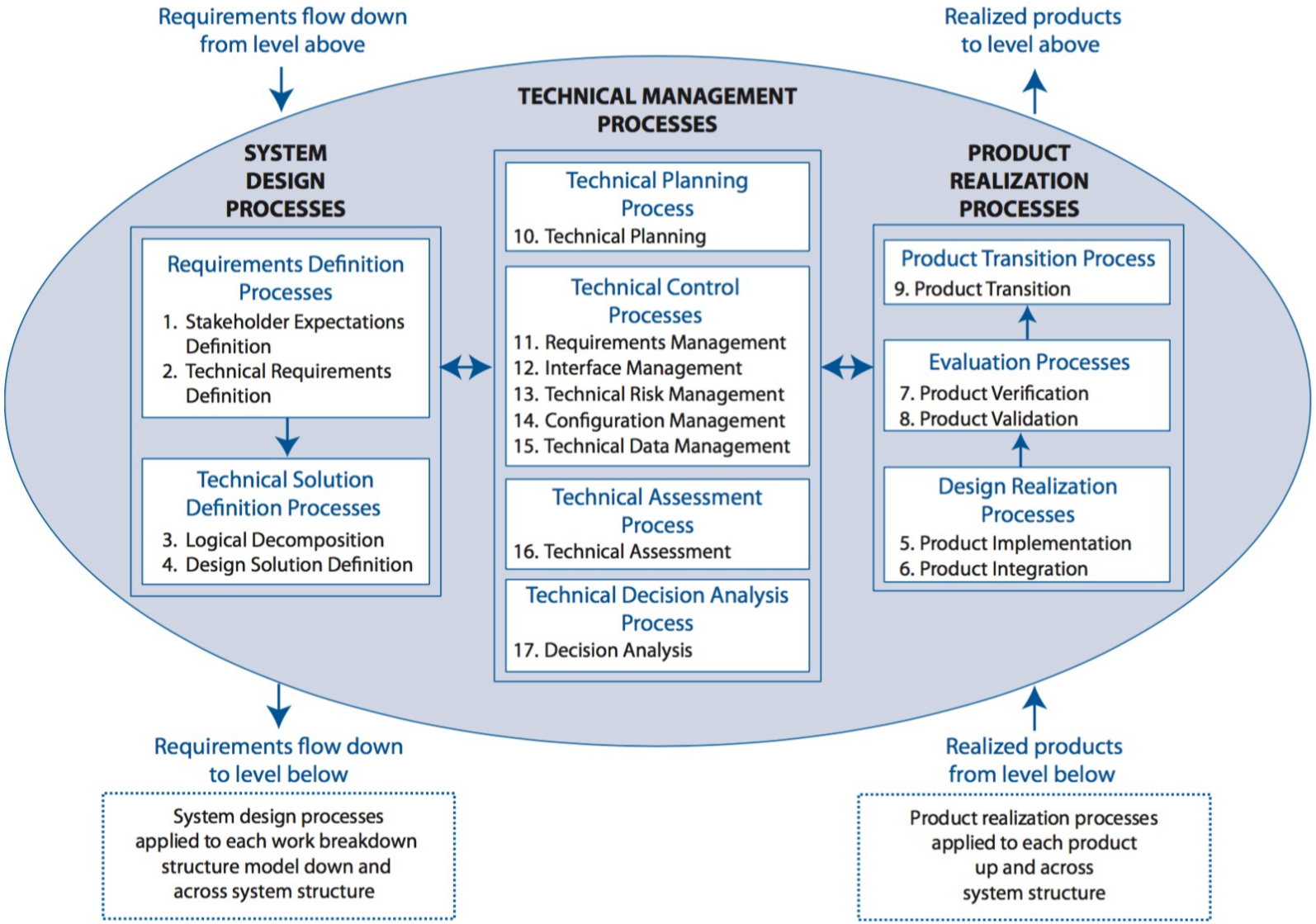


Figure 2.1-1 The systems engineering engine

NASA Project Process Flow

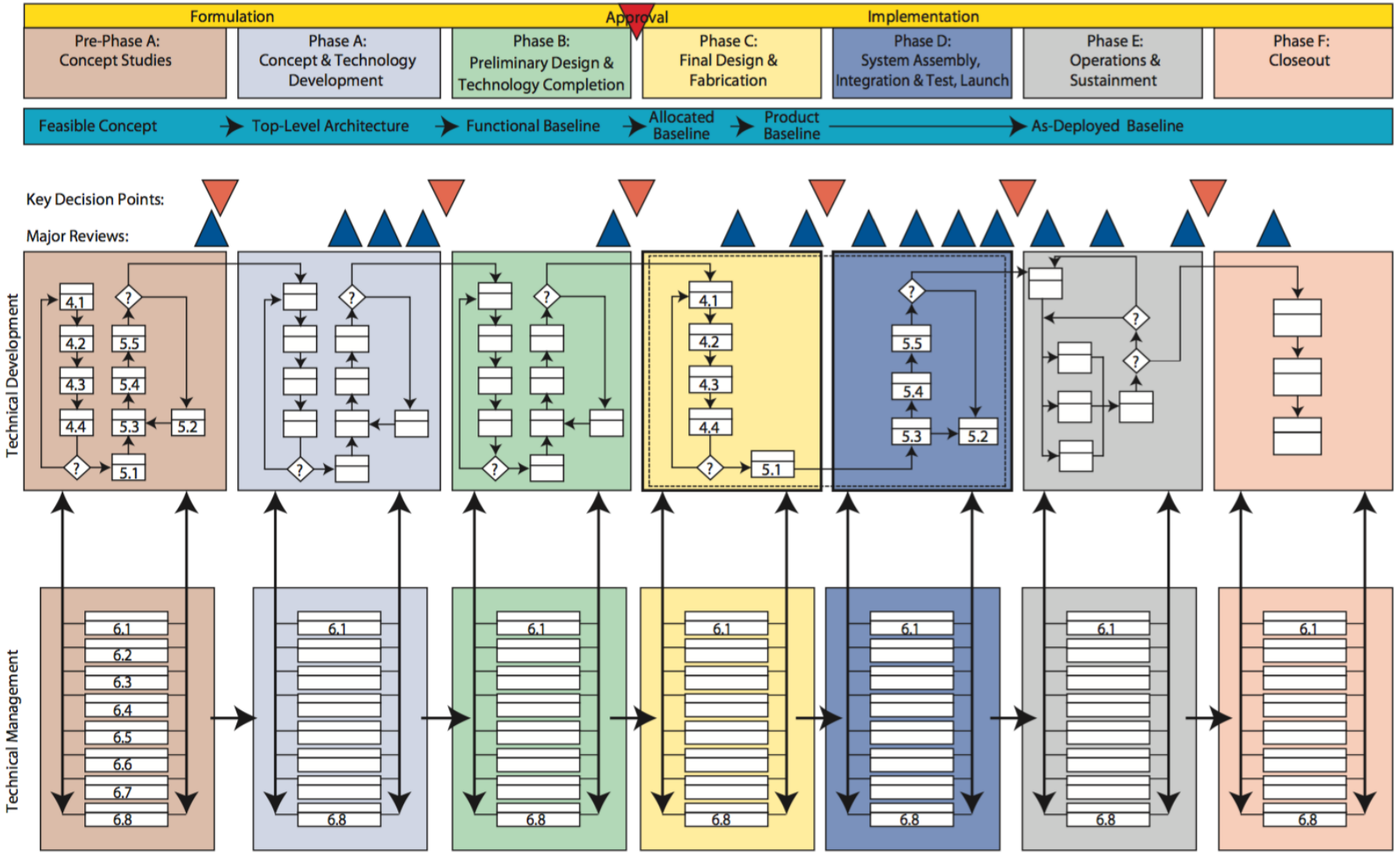


Figure 2.2-1 A miniaturized conceptualization of the poster-size NASA project life-cycle process flow for flight and ground systems accompanying this handbook

Table 2.3-1 Project Life-Cycle Phases

	Phase	Purpose	Typical Output
Formulation	Pre-Phase A Concept Studies	To produce a broad spectrum of ideas and alternatives for missions from which new programs/projects can be selected. Determine feasibility of desired system, develop mission concepts, draft system-level requirements, identify potential technology needs.	Feasible system concepts in the form of simulations, analysis, study reports, models, and mockups
	Phase A Concept and Technology Development	To determine the feasibility and desirability of a suggested new major system and establish an initial baseline compatibility with NASA's strategic plans. Develop final mission concept, system-level requirements, and needed system structure technology developments.	System concept definition in the form of simulations, analysis, engineering models, and mockups and trade study definition
	Phase B Preliminary Design and Technology Completion	To define the project in enough detail to establish an initial baseline capable of meeting mission needs. Develop system structure end product (and enabling product) requirements and generate a preliminary design for each system structure end product.	End products in the form of mockups, trade study results, specification and interface documents, and prototypes
Implementation	Phase C Final Design and Fabrication	To complete the detailed design of the system (and its associated subsystems, including its operations systems), fabricate hardware, and code software. Generate final designs for each system structure end product.	End product detailed designs, end product component fabrication, and software development
	Phase D System Assembly, Integration and Test, Launch	To assemble and integrate the products to create the system, meanwhile developing confidence that it will be able to meet the system requirements. Launch and prepare for operations. Perform system end product implementation, assembly, integration and test, and transition to use.	Operations-ready system end product with supporting related enabling products
	Phase E Operations and Sustainment	To conduct the mission and meet the initially identified need and maintain support for that need. Implement the mission operations plan.	Desired system
	Phase F Closeout	To implement the systems decommissioning/disposal plan developed in Phase E and perform analyses of the returned data and any returned samples.	Product closeout

Summary

- Method for developing, building, and maintaining systems safely.
- Systems are becoming more complex.
- Systems engineering aims to develop complex systems.
- Modeling and analysis based on it are important.

Summary

- Systems engineering also requires a process and associated management activities.

- Project management, i.e., the implementation of product development with regard to a given process, is also an important task.