32nd Annual INCOSE international symposium
hybrid event
Detroit, MI, USA
June 25 - 30, 2022

Oversimplification of Systems Engineering Goals, Processes, and Criteria in NASA Space Life Support

Harry Jones NASA Ames Research Center

www.incose.org/symp2022

Overview

- The standard systems engineering process has been oversimplified in space life support.
- Systems analysis demands slow, logical, and methodical thinking.
  - It is often bypassed in favor of quick, intuitive, subconscious “gut feel.”
- A study of 100 system designs found examples of 12 specific mental mistakes, such as ignoring stakeholder needs.
  - These mistakes are oversimplifications of the systems engineering process.
- An analysis of space life support found 11 examples of oversimplifications in systems engineering, such as neglecting safety and cost.
  - These 11 oversimplifications could be traced to the 12 previously identified mental mistakes or other well-known ones, such as ignoring sunk costs.
- Projects seem to be more guided by “gut feel” based on tradition, authority, and consensus than on the logical, rational systems engineering approach.

Introduction

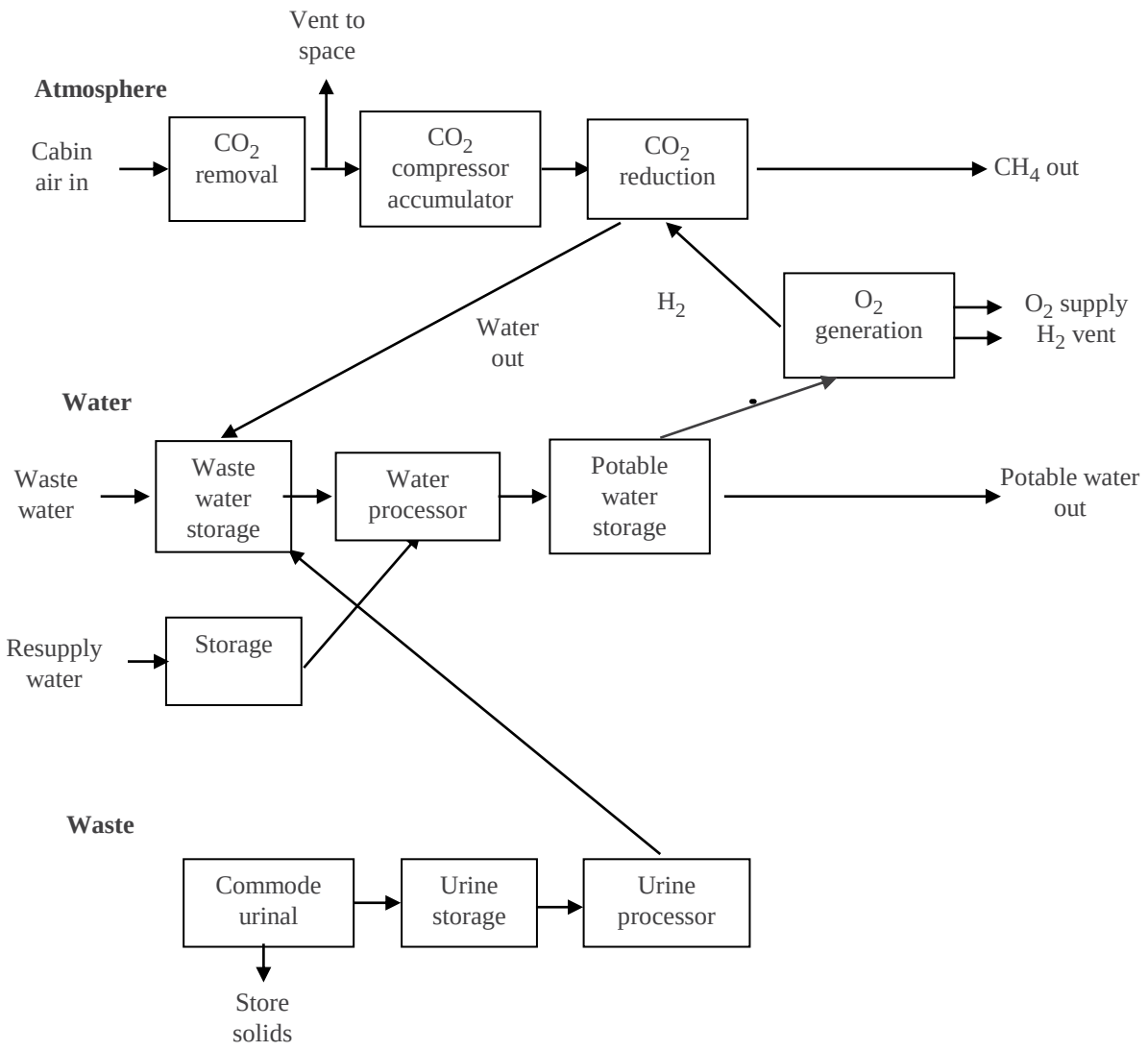
- The systems engineering process deals with complexity in two ways.
  - First, it designs a logical hierarchy of subsystems with reduced complexity.
  - Second, it follows a sequential development process from requirements through architecture, design, technology trade-offs, test, and customer validation.
- However, the full recommended systems engineering process is usually not completed.
  - The difficulty and cost of systems engineering grows with complexity.
  - Simplification occurs because of well-known cognitive limitations on memory span and working memory and by the propensity to use intuitive decision-making short cuts.
- In some cases, standard systems engineering can be seriously oversimplified.
  - The true system goals, the planned design effort, and the original trade-off criteria can be changed, reduced, or eliminated.

The Systems Engineering Process

#	Process
1	Requirements definition
2	Requirements flow down
3	Design options
4	Technology assessment
5	Systems analysis
6	Life Cycle Cost
7	Risk analysis
8	Safety analysis
9	System performance definition
10	Trade-offs and optimization
11	Integration
12	Test

- The requirements are based on the customer's needs.
- The requirements flow down defines the hierarchical system architecture.
- The design options are different implementations of the subsystems.

ISS Life Support



- Usual technology goals are improved performance, cost, and risk.
- Other life support goals are increased material closure and reduced launch mass.

Human cognitive limitations

- Psychological studies find serious limitations on the human decision processes and memory.
- Bounded rationality challenged the accepted idea of optimal rational decision making.
  - Both the available information and human analysis capabilities are limited.
  - Decision making with limited resources was called satisficing, not optimizing.
- Humans have limited short-term working memory of about 3 chunks.
  - This limit is not due to the inability to recall information.
  - Even with all the data provided, the relations between three or more variables cannot be easily understood.
- Systems designed by humans must be understood by humans.
  - The complexity of human designed systems is constrained by the limits on human cognition.

Use of Intuitive Methods in Decision Making

- In Daniel Kahneman's book, Thinking, Fast and Slow, he explains that humans use two modes of thinking.
  - System 1 is quick, intuitive, and unconscious. Used when the problem is familiar and the decision obvious. Usual.
  - System 2 is slow, conscious, and focused. Used when a problem appears complex and difficult to solve. Rare.
    - Systems engineering is rational system 2 thinking.
- System 1 jumps to conclusions using heuristics.
  - A heuristic is an instinctive rule-of-thumb that solves problems quickly.
    - They can produce systematic errors in decision making.
  - Heuristics include anchoring, attribute substitution, availability, framing, loss aversion, overconfidence, and the sunk cost fallacy.

12 Mental Mistakes in Systems Engineering

- A two-decade study of more than 100 engineering designs found examples of 12 different mental mistakes.
- They are using dependent criteria, not stating the problem in terms of stakeholder needs, vague problem statement, substituting a related attribute, sensitivity analysis mistakes, using traditional unexamined criteria, weight of importance mistakes, anchoring on first suggestion or the status quo, treating gains and losses equally, not using scoring functions, implying false precision, and ignoring expert opinion.

Mental Mistakes in Life Support Engineering

#	Mental Mistake
5	Substituting a Related Attribute
4	Not Stating the Problem in Terms of Stakeholder Needs
3	Not Using Scoring Functions
2	Anchoring to the Status Quo
1	Ignoring Expert Opinion
1	Using Traditional Unexamined Criteria
1	Not Ignoring Sunk Cost (New)
1	Overconfidence (New)
1	Using System 1 Rather Than 2 (New)

- 19 instances of mental mistakes were found.
- They were of 9 different types.
  - 6 were in the 12 found earlier.
  - The missing 6 concern defining and weighting criteria.
    - This was not formally done.
- The 3 others are well known but not previously listed.

Example Mental Mistakes in Life Support 1

- Recycling life support research was justified as needed to increase material closure and reduce launch mass, rather than improving performance, cost, and risk.
  - Attribute substitution, not stakeholder needs
- Considering only improved ISS life support for transit to Mars.
  - Anchoring to the status quo, not ignoring sunk cost
- Using a launch mass metric alone to select technology.
  - Attribute substitution, using traditional unexamined criteria, not using scoring functions (for all criteria)

Example Mental Mistakes in Life Support 2

- TRL (Technology Readiness Level) is used to screen R&D.
  - Attribute substitution, anchoring to the status quo, not ignoring sunk cost, not using scoring functions (for all criteria)
- Standard systems engineering replaced by management intuition and group consensus.
  - Intuitive system 1 rather than analytic system 2.

Example Mental Mistakes in Life Support 3

- Probabilistic risk analysis (PRA) replaced by one or two fault tolerance, which may not improve reliability.
  - Attribute substitution (redundancy for reliability)
- 10's of hours of ground testing of ISS before 10's of years service.
  - Ignoring expert opinion, overconfidence

How Is Systems Engineering Oversimplified?

- The intuitive methods and mental models used to oversimplify systems engineering are widely used in decision making.
  - Oversimplification seems completely natural and reasonable.
- Even though it seems to be widespread and damaging, oversimplification of the systems engineering process has not been identified as a problem.

System failures are often due to systems engineering causes

#	Failure Cause
32	Design and design test
26	Manufacturing and manufacturing test
19	Program and systems engineering management
8	Software and software test
5	Policy, cost, and schedule
4	Planning

"Anything less than the full measure of systems engineering rigor will expose the project to failure."

- A systems engineering analysis found 94 failure causes in 50 different space systems.
- About 20% were due to program and systems engineering management.

Why is oversimplification accepted?

- The standard systems engineering process should prevent oversimplifications and correct mental mistakes.
  - Critical reviews should detect errors.
- Oversimplification is accepted because the expected logical systems engineering process is neglected in favor of a more intuitive reliance on past tradition, management authority, and group consensus.

Pragmatic American Philosophy

- In 1877 Charles Sanders Peirce described the four methods that people use to determine their beliefs:
  - tradition,
  - authority,
  - consensus, and
  - reason.
- Reason is the scientific method.
  - Reason is the only method that admits it can make mistakes.
  - Reason is the only method that criticizes and tests itself.
  - Reason is the only method designed to find the truth rather than agreement.

Tradition, Authority, and Consensus Have Been Used to Oversimplify Space Life Support

- The design of the ISS life support system is traditional.
  - A 1960's human closed chamber test of life support used similar architecture and technology.
  - Five decades of engineering progress, such as in control and automation, have not been incorporated in life support design.
- Life support management has exercised authority.
  - A mass metric was made the major technology selection metric.
  - Improved ISS life support was endorsed for transit to Mars.
- A life support community consensus has supported most of the oversimplifications mentioned here.

Conclusion

- The systems engineering process has been drastically oversimplified in space life support.
- Management often has an urgent need for optimistic project advocacy.
  - Systems engineering analysis of potential problems can draw attention to difficulties and create a negative impression.
  - Favorable assumptions can be preferred to realistic analysis.
- The compelling reason for oversimplifying systems engineering may be to avoid the damaging impact of a realistic assessment of project issues.

32nd Annual INCOSE international symposium

hybrid event

Detroit, MI, USA
June 25 - 30, 2022

www.incose.org/symp2022