L3HARRIS™

APPLYING DECISION ANALYSIS TO A SAFETY CRITICAL SYSTEM: *CHOOSING A SERVICE ORIENTED ARCHITECTURE TO REPLACE A LEGACY MONOLITH*

July 30, 2019 Nicolas H. Malloy, Systems Engineer, Northampton, MA, United States

Overview

- For this design decision we consider a legacy system with a monolithic architecture.
  - A monolithic architecture is the traditional unified model for the design of a software program.
  - This kind of architecture is designed to be self-contained; components of the program are interconnected and interdependent (WhatIs, 2016).
- The system under analysis is a Safety Critical (SC) naval combat system that provides weapon and attack control functions and the initiation and control of the weapon launch for both tactical and defensive weapons.

Approach

Michael Frank's Seven Steps for a formal decision analysis:

Decision Analysis is a systematic, quantitative and visual approach to addressing and evaluating important choices.

The seven steps for a formal decision analysis process outlined in Franks' book, Choosing Safety are as follows:

- Identify a Decision Opportunity
- Create a Problem Statement
- State the Objective and Attributes
- Create Alternatives
- Develop a Decision Model
- Develop a Value Model
- Synthesize Decision and Value Models to Rank Alternatives (Frank, 2008).

Identify a Decision Opportunity

- Problem
  - Code maintenance issues plague the current system design.
  - Just about every time code maintenance is performed a new issue resulting from the maintenance is later discovered. The issues are software bugs.
- Impact
  - These bugs cause schedule delays and unplanned increases to program cost.
  - There have been several instances where bugs have affected SC system functionality.
  - If such a bug were to cause the inadvertent launch of a weapon the consequences could be catastrophic.
- Opportunity
  - Determine how these code maintenance issues can be alleviated using a Service Oriented Architecture (SOA).

Identify a Decision Opportunity (cont.)

Monolithic Architecture vs. SOA Architecture

(InfoPulse, 2018.)

Create a Problem Statement

- Updating the monolithic system carries the risk of creating bugs which impact safety, schedule, and cost.
  - When software engineers receive a Problem Report they make changes to the code to fix it.
  - Sometimes when changes are made to the code there are dependencies on that code that exist elsewhere in the system.
  - If dependencies are not fully understood when the changes are committed to the build the result can be a software build with bugs.
  - When dealing with a SC system one bug can cause a lot of problems.

State the Objective and Attributes

- The objective of this decision analysis is to analyze the options and identify the safest, most maintainable, and cost effective architectural design for the combat system.
- There are three attributes that will be measured:
  - *Safety*
  - *Cost*
  - *Maintainability*

Table 1 Attributes and Weighted Values

Alternative	**Safety**	**Cost**	**Maintainability**
Baseline Goals	JSSSEH Compliant and strong type programming	<$1,000,000	Is There Low Risk in Modifying the Code?
Weighted Value	0.50	0.30	0.20

Create Alternatives

- Alternative 1: Re-architect the system with a service based approach from the ground up using C++ language.
- Alternative 2: Re-architect the system with a service based approach from the ground up using Ada language.
- Alternative 3: Modularize the existing system such that each module performs a specific service and thus retains the current Ada language.

Table 2 Objectives and Attributes

Alternative	**Safety**	**Cost**	**Maintainability**
Baseline Goals	JSSSEH Compliant and strong type programming	<$1,000,000	Is There Low Risk in Modifying the Code?
Weighted Value	0.50	0.30	0.20
Alternative 1	No	$1,000,000	Yes
Alternative 2	Yes	$1,000,000	Yes
Alternative 3	Yes	$750,000	Yes

Develop a Decision Model

- The decision model was based off alternatives, attributes, and the outcomes of those attributes as they pertained to the alternatives.
- By taking this approach, it was possible to derive a measurable result that can later be used in the value model.

Table 3 Decision Model Scoring

Alternative	Safety	Score 1	Cost	Score 2	Maintainability	Score 3
Baseline Goals	JSSSEH Compliant AND Strong Data Type	-	<$1,000,000	-	Is There Low Risk in Modifying the Code?	-
SOA using C++	No	0	$1,000,000	0	Yes	1
SOA using Ada	Yes	1	$1,000,000	0	Yes	1
Modularize Existing Arch Retaining Ada	Yes	1	$750,000	1	Yes	1

Develop a Value Model

- The decision model was based off of alternatives, attributes, and the outcomes of those attributes as they pertained to the alternatives.

Table 4 Weighted Scoring of Attributes Value Model

Attribute	**Alternative 1**	**Weighted Score 1**	**Alternative 2**	**Weighted Score 2**	**Alternative 3**	**Weighted Score 3**
Safety	0	0	1	0.50	1	0.50
Cost	0	0	0	0	1	0.30
Maintainability	1	0.20	1	0.20	1	0.20
Weighted Value	-	0.20	-	0.70	-	1.0

Synthesize Decision and Value Models to Rank Alternatives

- Decision Synthesis
  - Alternative 3 met all three of the design attributes captured in the decision and value models.
  - In terms of safety Alternative 2 and 3 met the criteria while Alternative 1 did not.
  - Alternative 3 met the desired cost while Alternatives 1 and 2 did not.
  - Alternatives 1, 2, and 3 presented maintainable approaches for the system architecture. Whether the system is being re-architected or modularized from an existing code base the maintainability will improve. Each system would be expected to exhibit fewer bugs than the legacy monolithic design.

Synthesize Decision and Value Models to Rank Alternatives (cont.)

- The final ranking of the proposed alternatives based on the derived weighted scores is as follows:
  - Alternative 3 received a weighted score of 1.0
  - Alternative 2 received a weighted score of 0.70
  - Alternative 1 received a weighted score of 0.20

Table 4 Weighted Scoring of Attributes Value Model

Attribute	Alternative 1	Weighted Score 1	Alternative 2	Weighted Score 2	Alternative 3	Weighted Score 3
Safety	0	0	1	0.50	1	0.50
Cost	0	0	0	0	1	0.30
Maintainability	1	0.20	1	0.20	1	0.20
Weighted Value	-	0.20	-	0.70	-	1.0

Decision Analysis Summary

- The decision analysis identified Alternative 3 as the best architectural approach for improving code maintenance by making the code base more easily maintainable.
- Alternative 3 will:
  - Use an architectural approach that is compliant with the JSSSEH.
  - Be the cheapest approach to creating a SOA.
  - Result in a system that carries lower risk for code modifications.
    - Once the system has been modularized it will reduce the likelihood of code changes affecting other areas of the system.
    - System Testing will focus on impacted portions of the system

Conclusion

Decision Analysis is a straightforward method to the decision making process. Below are some of the Benefits and Disadvantages to the Michael Frank's Seven Step approach.

Benefits

- **Methodical Process.** Clearly defining a situation and stating the required outcome can go a long way towards improving a situation. (Decision Making Confidence, 2019)
- **Encourages Research.** Often gives rise to options previously not considered or may even generate options in regard to other unrelated decisions. (Decision Making Confidence, 2019)
- **Clearly Defines the Problem.** Well-defined problems lead to breakthrough solutions. When developing new products, processes, or even businesses, most companies aren't sufficiently rigorous in defining the problems they're attempting to solve and articulating why those issues are important. (Spradlin, D., 2012)

Challenges

- **Having too Much or Not Enough Information.** Gathering relevant information is key when approaching the decision making process, but it's important to identify how much background information is truly required. (Hussung, T., 2017)
- **Misidentifying the Problem.** In many cases, the issues surrounding your decision will be obvious. However, there will be times when the decision is complex and you aren't sure where the main issue lies. Conduct thorough research and speak with internal experts who experience the problem firsthand in order to mitigate this. (Hussung, T., 2017)
- **Overconfidence in the Outcome.** Even if you follow the steps of the decision making process, there is still a chance that the outcome won't be exactly what you had in mind. That's why it's so important to identify a valid option that is plausible and achievable. Being overconfident in an unlikely outcome can lead to adverse results. (Hussung, T., 2017)

Connect With Me

Medium

https://medium.com/@nicolasmalloy

Linkedin

www.linkedin.com/in/nicolasmalloy

Acknowledgements

- Michael Cuff, Sr. Systems Engineer, Northrup Grumman
- Tim Marcinowski, Founder, YetiCloud

References

Activity, N. O. (2012). Joint Software System Safety Engineering Handbook. Washington D.C.

Architecture, S. (2017, 11 13). Service-Oriented Architecture (SOA) Definition. Retrieved from Service Architecture: https://www.service-architecture.com/articles/web-services/service-oriented_architecture_soa_definition.html

Frank, M. V. (2008). Choosing Safety: A Guide to Using Probabilistic Risk Assessment and Decision Analysis in Complex, High-consequence Systems. Washington, DC: Resources for the Future.

Harbeck, R. (1999, 12 3). Strongly Typed. Retrieved from TechTarget: http://whatis.techtarget.com/definition/strongly-typed

WhatIs. (2016, May). Monolithic Architecture. Retrieved from WhatIs: http://whatis.techtarget.com/definition/monolithic-architecture

InfoPulse. (2018, November). The Importance of Microservices Architecture for Modern Applications: https://www.infopulse.com/blog/the-importance-of-microservices-architecture-for-modern-applications/

Spradlin, D. (2012, September). The Power of Defining the Problem: https://hbr.org/2012/09/the-power-of-defining-the-prob

Hussung, T. (2017, February). 7 Steps of the Decision Making Process: https://online.csp.edu/blog/business/decision-making-process

Decision Making Confidence. (2019). Six Step Decision Making Process: https://www.decision-making-confidence.com/six-step-decision-making-process.html