Architecting as a Means of Bounding Risk in the Future

Kenneth J Kepchar
Federal Aviation Administration
Kenneth.kepchar@faa.gov

Abstract. Traditional architecture development efforts have deferred most risk considerations until after the functional architecture has been established and the imbedded concepts are being turned into operational solutions. This paper discusses a framework that moves Risk Management "upstream" and integrates it into the architecture development process. Including risk management at the architectural development stage provides early insight into the delicate balancing act between the benefits anticipated vs. risks incurred in selecting (or not selecting) features of candidate architectures to address stakeholder needs driving the scope and context of the architectural choices. Thus, application of risk management during architectural development provides a proper balance between risk and opportunity, avoids potential unacceptable risks where appropriate, and takes a proactive and well-planned role in anticipating and responding to risks prior to implementation.

Background. Architecting is about shaping the future. Because the future involves a great deal of uncertainty, risk is a natural component of any architecting effort. An architecture embodies a structure, a set of relationships, and principles linked to accomplish a purpose. In other words, an architecture establishes a pattern and balance of major elements within some context or environment, shapes behavior through a set of interface relationships, and provides a framework to make decisions.

Risk Management Framework. The objective of Risk Management is to deal with uncertainty while providing a proper balance between risk and opportunity. It seeks to understand the potential risks to an endeavor, and to take a proactive and well-planned role in anticipating them and responding to them if they occur. **Risk is defined as a future event or situation with a realistic (non-zero nor 100 percent) likelihood/probability of occurring and an unfavorable consequence/impact to the successful accomplishment of well-defined goals if it occurs.** Any architecture development effort should include a Risk Management process designed to provide a proper balance between risk and opportunity, avoid potential unacceptable risks where appropriate, and take a proactive and well-planned role in anticipating and responding to risks as they occur. Using a disciplined Risk Management framework for architecture development (Figure 1) provides an organized, systematic decision-making methodology to effectively deal with uncertainty in accomplishing the objectives defined for that architectural effort.

The use of this Risk Management process during the development of an architecture has three primary objectives:

1. Inclusion of risk in the architectural assessment framework ensures that the concepts and courses of action with extreme risk are generally avoided and/or filtered out of the various architectural features generating these risks as they are identified. Alternatively, subsequent composite architectures that are developed to evaluate the features are designed specifically to eliminate or mitigate such risks.
2. Risks which remained in the preferred Architecture are considered when developing recommendations, in many cases including focused research,

development, or assessment designed to mitigate such risks, vice immediate implementation of a high risk feature.

3. The residual risks are documented in the final architecture report, and should be considered for further mitigation during follow-on activities such as implementation planning.

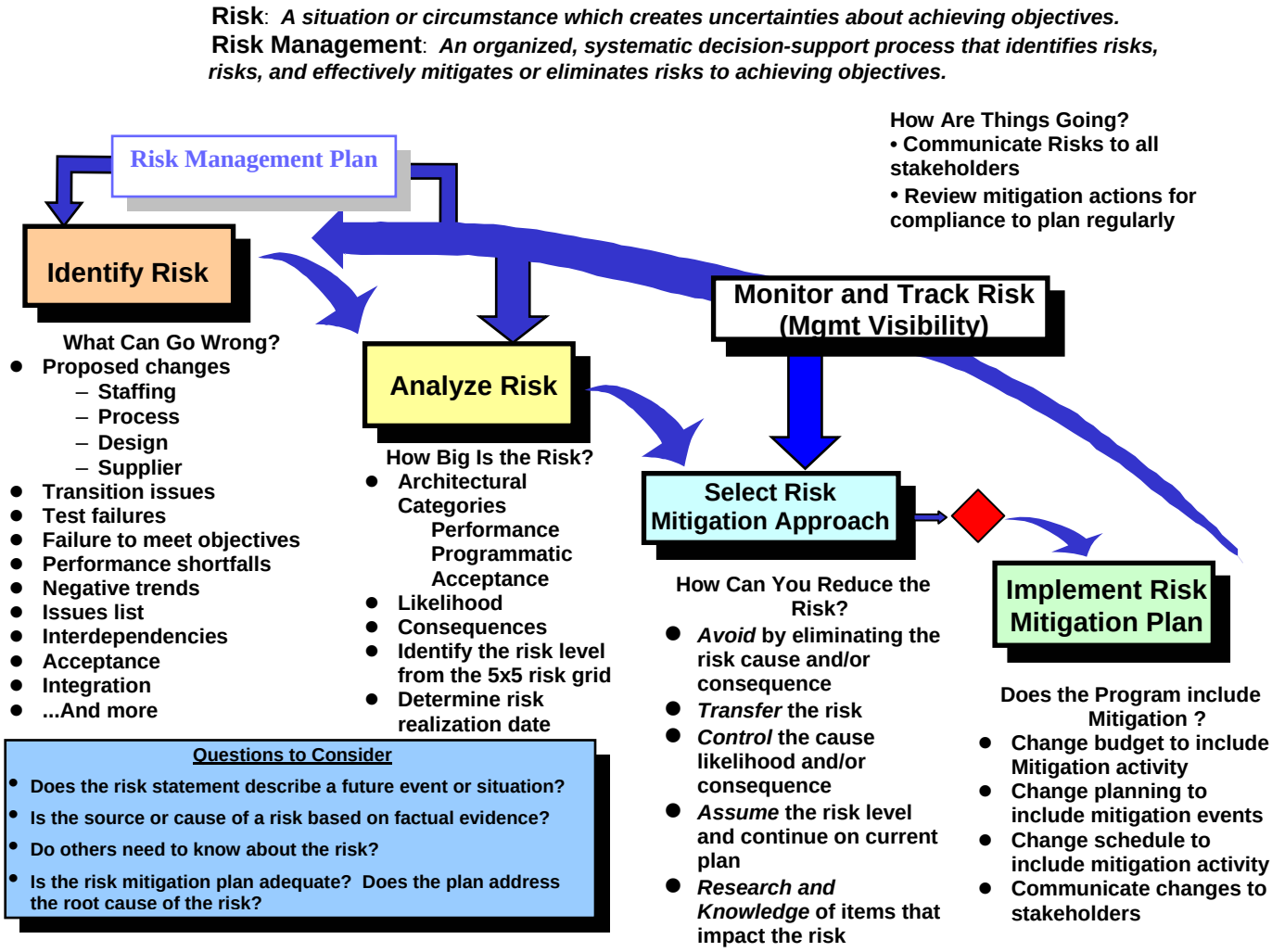


Figure 1 – Risk Management Framework

Risk Identification. Risk identification is a systematic effort to uncover possible events or conditions that, if they occur, may hinder achievement of program or organization objectives. As the characteristics or features of a number of representative architecture are explored, any accompanying risks were identified. A risk log is developed and the risks grouped into 3 major categories driven by root cause, usually performance, schedule, and cost.

Risk Analysis. Risk analysis or risk assessment provides program insight into the significance of identified risks. Risk analysis attempts to assess the likelihood of identified risks and the consequence to the endeavor if the risk event or condition occurs. The process also classifies each risk according to the root cause of the risk event (cost, schedule, or technical performance). Risk analysis assesses each of the two components of an identified

risk — (1) the likelihood of the risk occurring, and (2) the consequence to the program if it occurs.

Risk Mitigation. The objective of risk mitigation or risk reduction efforts is to implement appropriate and cost-effective risk mitigation plans to reduce or eliminate the risks. Appropriate risk mitigation techniques are selected and mitigation actions are developed, documented, and implemented. Risk mitigation handling (planning, implementation, and tracking) is the core of risk management.

Mitigation Implementation. Once the organization decides on a risk mitigation approach and supporting actions, the decision shall be implemented and carried out effectively so that either risk likelihood or consequence, or both, are reduced to an acceptable level.

Mitigation Monitor & Track. Because risk is dynamic, continual attention of all involved is necessary regarding how the risk profile is changing based on events, decisions, and actions on the project. Reassessing currently managed risks is done on both a periodic and event basis to reflect current status of the risks as well as to identify and quantify new and emerging risks. New potential risks to the program may be identified at any time. Newly identified risks are analyzed using the same steps described above.

Risk Framework in the Architectural Context. A traditional view of risk frameworks classifies each risk according to the root cause of the risk event, typically in the categories of technical, schedule, and cost.. While these dimensions are useful and easy to understand, they need to be tailored to make the discussion of risk meaningful in an architectural setting. For, example, the main drivers of an architecture will be the "performance based" features of the solution. In other words, the degree of utility of the final recommended architecture is its functionality and extent that it satisfies the stakeholder's needs. For the purposes of supporting the development of an architecture, it is more useful to view the root cause in terms of (1) **performance** of the capabilities captured in the architecture, (2) **programmatics** of implementing the recommendations, or (3) external forces such as stakeholder **acceptance** that influence the realization of the architectural components.

The **performance category** deals with the characteristics and features of the architecture itself: It considers performance benefits offered by inclusion of a capability in the architecture, as well as the performance uncertainties introduced as a result. This category looks at such considerations as technical capabilities, integration issues, technologies involved along with their maturity levels, and operational considerations, as shown below.

Performance
Technology (TE)
Integration (IN)
Technical Capabilities (Tx)
Hardware (TH)
Software (TS)
Sci/Eng Algorithms (TA)
Operational Problems (OP)

Figure 2 - Performance risk aspects

To aid in a subsequent risk analysis, the aspect(s) of performance potentially driving the risk are identified as components or functional building blocks that are incorporated during development of candidate architectures.

Implementing specific features of an architecture impose a set of uncertainties, usually driven by the **programmatic efforts** to turn the architectural concepts into actual capabilities or systems. More traditional categories of implementation/transition, schedule, and cost provide useful insight into the risks associated with this phase of the endeavor as shown in Figure 3.

Programmatic
Cost (PC)
Schedule (PS)
Implementation/Transition (PI)

Figure 3 - Programmatic risk aspects

Acceptance captures those conditions and forces external to the architecture that influence the extent that concepts in the architecture become part of the actual operational system or product. This category includes consideration of the impacts on the stakeholder and user, within political, international, social, market, and policy contexts.

Acceptance
Stakeholder Participation (AS)
User (AU)
Policy (AP)
International (AI)
Ownership (AO)
Economic/Social (AE)
Military Pre-eminence (AM)

Figure 4 - Acceptance risk aspects

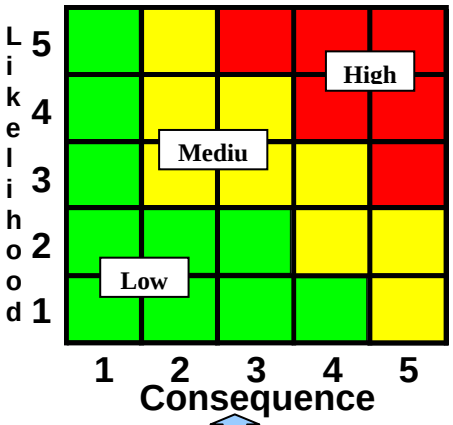
A likelihood (probability) template is developed that applies to the architecture(s) under analysis. The established criteria are based on the premise that any architecture will be integrated with existing solutions to some extent. Rare is the opportunity for an architect to start will a blank sheet, especially when the environmental context of the final solution is factored into the equation. Another set of templates was used to evaluate consequence/impact to the effort if the risk materializes. Again, the established criteria is driven by the objectives in creating the architecture itself. For, example, if the architecture under consideration involves national goals or priorities, then the acceptance (category) would be based on national goals and objectives. If the stakeholder is a manufacturing organization, then the objectives would be expressed in terms of the organizational mission statement or similar goals.

The likelihood and consequence are considered to be independent, but are tied to the same event. They are mapped into a risk grid to determine the individual risk level (e.g., high (red), medium (yellow), or low (green)) as shown in Figure 5. The general criteria shown in the Figure are tailored to support the objectives driving the architecture.

Architecture Risk Assessment Criteria and Grid

What is the Likelihood the risk will happen?

Likelihood			Existing Infrastructure, Governance and
Level			
5	Near Certainty	… cannot integrate into existing infrastructure. (>90% chance it WILL happen)
4	Highly Likely	…Major infrastructure changes required. (>2/3 chance it WILL happen)
3	Likely	… Changes to (existing) infrastructure required. (~50% chance it WILL happen)
2	Low Likelihood	…some infrastructure changes required to accommodate. (<1/3 chance it WILL happen)
1	Not Likely	…easily integrated into (existing) infrastructure. (<10% chance it WILL happen)



Given the risk is realized, what would be the magnitude of the impact?

Consequence	Performance	Programmatic	Acceptance
Level			
1 – *No impact to Architecture*	Minimal	Minimal	Minimal
2 – *Negligible impact to Architecture success*	Minor performance same approach retained	Development/acquisition Cost/schedule increase ≤	Minor variation from stakeholder objectives
3 – *Limited impact to Architecture objectives*	Moderate performance ...alternatives available	Development/acquisition increase >1% ≤ 5%	Requires modification to support objectives
4 – *Success could be jeopardized*	Unacceptable performance but alternatives available	Development or acquisition increase >5% ≤10%	Major changes required to support objectives
5 – *Success in doubt*	Unacceptable performance and NO alternatives exist	Development or acquisition increase >10%	No longer compatible with objectives

Figure 5 – Architecture Risk Grid for Determining Risk Level

Architecture Process. Architectures occur at many levels ranging from the simple to extremely complex. We're all familiar with architectures related to designing a building or a city. However, architectures are just as evident in the structure of an insect, a spacecraft, or an Air Transportation Management System. Every architecture should contain the following:

1. A set of assumptions about the future environment portrayed by the architecture.
2. A set of time dependent states of view, typically the present, future (end state), and a point of transition
3. A set of concepts
4. Benefits and costs related to these concepts
5. Recommendations to realize the future state portrayed

Developing architectures is often more an art than a science. However, architecting as a process can be characterized as occurring in four (4) basic phases[1]:

1. Data Gathering – Identifying needs & gaps, current environment, technologies, and existing solutions/systems

[1] 1. National Position, Navigation, and Timing (PNT) Architecture Final Report, National Space Security Office (NSSO), September 2008

2. Concept Development – Establishing trade space attributes and potential concepts to be evaluated, which are grouped into candidate "architectures" to explore potential solution "themes" or "vectors"
3. Analysis & Assessment – Assessment of attractive or salient features of alternate architectures within an analytical framework to support development of composite or "hybrid" architectures
4. Recommendations – Formulation of conclusions and recommendations in the form of a recommended architecture

Data Gathering. "Data Gathering" collects information relevant to task of developing an architecture for a future timeframe. This information includes:

1. projections on the future environment in which the architecture will operate;
2. current requirements and projected future needs;
3. current technology assessments;
4. current baseline systems, capabilities, and their projected future state if no new architecture is developed;
5. cost basis information needed for architectural cost projections;
6. currently identified capability gaps; and
7. information from the market , both public and private sectors.

The purpose of data collection is to develop an appreciation of the required functions, objectives, and trade space drivers before beginning to explore potential alternative futures. The risks associated with current systems and practices are well known, though not always widely recognized, or in extreme cases ignored. Otherwise, how do we explain the widespread failure of so many financial risk models that are contributing to the current economic malaise sweeping the globe?

Concept Development. Concept development builds on the Data Gathering effort to create an architecture, and comprises two major activities: development of the architectural trade space, and the synthesis, development, and assessment of candidate architectures used to gain insight into different aspects of that trade space.

A set of descriptive trade axes are developed to define the architectural trade space and differentiate between architectural concepts. The trade axes used can either be "descriptors" that describe the types of solutions being considered or "evaluators," such as cost and performance, commonly used in systems engineering to evaluate and compare interactions between solutions.

Architectural concepts are general descriptions of material and non-material solutions. They may be, but are not necessarily, linked to specific needs or existing implementation solutions, since these needs and solutions have not been identified for some future timeframe, say 2015, 2025, or 2050; however, they must be relatable to the architectural trade axes. A set of predefined architectural concepts are placed within the trade space according to their characteristics and evaluated against the trade axes as illustrated in Figure 6. As the characteristics of the concepts are identified, so are the risks associated with each concept. This approach helps ensure that combinations of various "outside the box" approaches have been considered and possible solutions in all the "corners" of the architectural trade space have been explored.

Candidate architectures (CA) are developed and evaluated to characterize and gain insight into the strengths, weaknesses, and architectural features associated with different areas of the architectural trade space. A set of objective criteria must be defined and developed to evaluate candidate concepts and the degree that each meets the stakeholders' needs. This helps ensure the architects do not rush to an apparently obvious solution without considering the full range of available options, and the implications of using solutions from different areas of the trade space. The ability of a candidate architecture to meet potential needs is not as important in the early stages of architectural development as increasing the understanding of why an architectural elements would meet (or not meet) those needs or why architectural elements would inhibit (or enable) other architectural elements in meeting those needs. Elements associated with the candidate architecture's trade space "corner" or "edge" are selected to be included. This approach results in extreme solutions that allows the strengths and weaknesses associated with different architectural approaches to be identified.

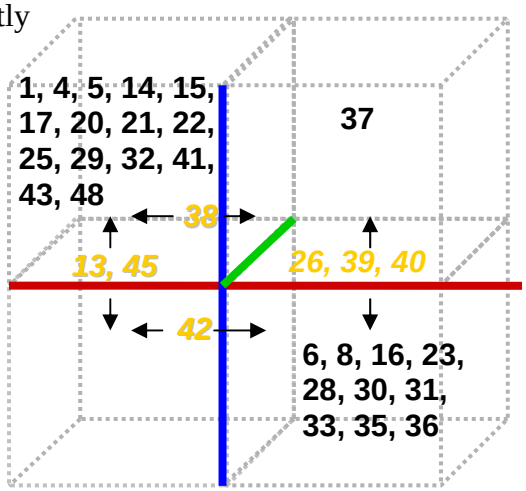


Figure 6 – Concept Placement Within the Trade Space

The results of the trade space evaluation are used to create a number of candidate architectures that explore aspects of trade space, where each candidate architecture is an intentional and significant departure from the solutions as we know them today, as shown in Figure 7. The team in turn evaluates the features of each candidate concept to develop and assess which would be suitable candidates for inclusion in hybrid architectures that span the trade space. The candidate architectures are developed and evaluated with the primary objective of obtaining insights, finding trends, and identifying key features that could be used to develop the "rational middle" blend of concepts in what are termed "hybrid architectures". The expected ability of each CA to meet user needs, satisfy identified gaps, and address the evaluators being used for the analysis are key factors at this stage of architectural development.

- **Purpose of building a CA is to explore the trade space**
- **Evaluate each CA to identify features that prove useful to meeting needs and eventually become recommendations**

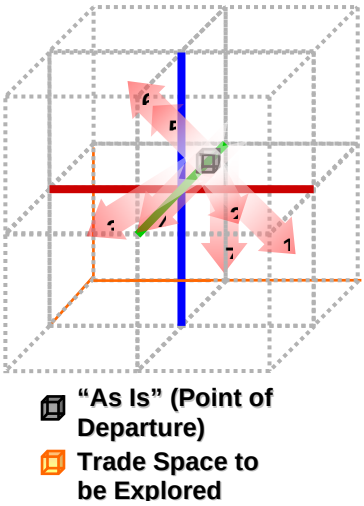


Figure 7 – Candidate Architectures

The candidate architectures reflect an intentional and significant departure from the future state of today's systems as a means to explore the positive and negative aspects of specific regions of the trade space. Hybrid architectures are intended to explore a more rational integration of concepts which span the trade space in response to stakeholder needs.

Risks are identified and a preliminary analysis is performed throughout the development of the candidate architectures based on subject matter expert (SME) perspectives on the risks associated with the concepts in each CA.

However, architects are not typically trained in risk identification or analysis. To allow the architects to focus on the task at hand, some simple job aids are essential to avoid risk discussions becoming a distracter to the overall architecture evolution. To assist with the data gathering, a template for risk identification should be used. An example of one recently used by the author is shown in Figure 8.

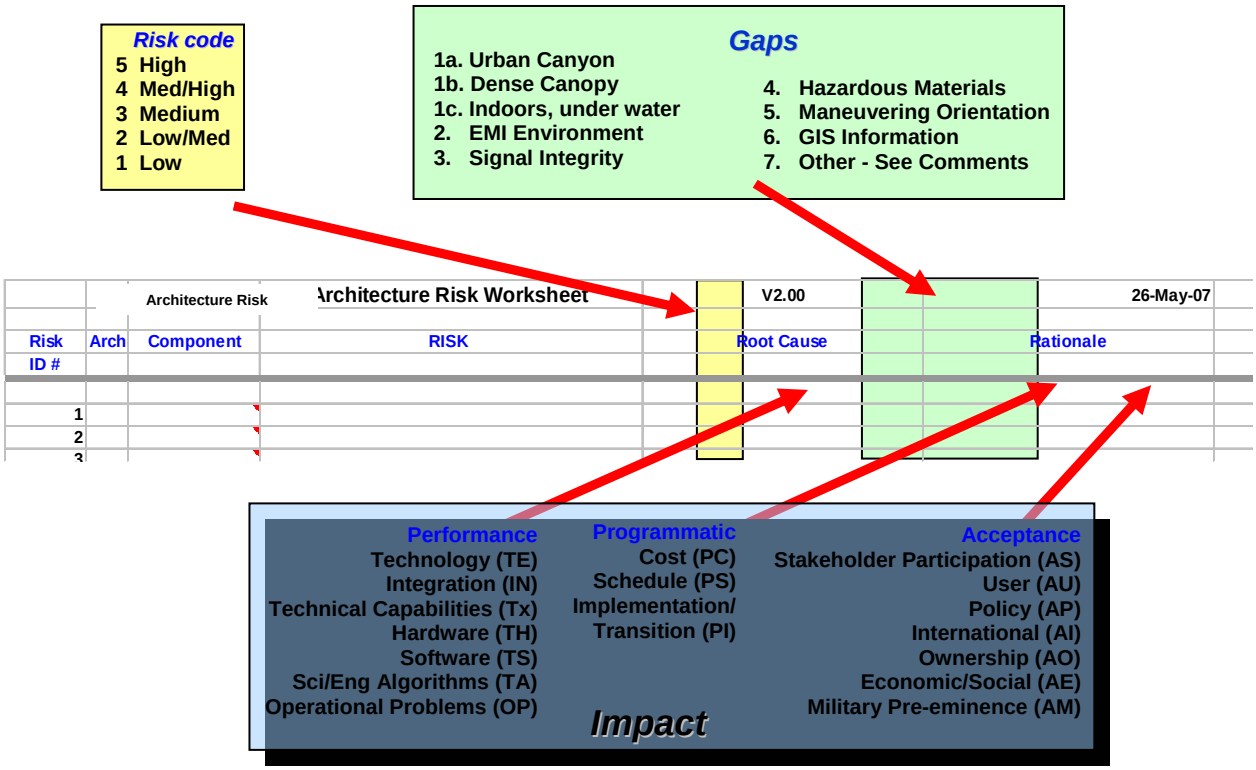


Figure 8 –Architecture Risk Data Gathering Template

The participants were requested to relate areas of uncertainty to the gaps that served as the basis for the architecture development. This data is compiled into a risk register and summarized. The summarized risks help drive the final "Should Be" recommendations, which in-turn help mitigate the risks identified.

The 2nd step in the process framework in Figure 1 is to perform an assessment of each risk to determine its relative impact on the overall architectural effort. A preliminary analysis is performed on the identified risks on all concepts being considered to ensure a degree of consistency on the relative assessment ratings across the architecture. Detailed analysis of the individual risks is deferred until a later stage in the process.

Analysis and Assessment. Having investigated fundamental trades central to the stakeholder needs driving the architectural effort, hybrid architectures are developed to satisfy user needs

and overcome capability gaps. The integrated concepts in each hybrid are designed to support a "theme" to meet future needs, overcome capability gaps, and support political, economic, and military strategies in a risk- and cost-informed manner. For example, in safety of life aviation navigation situation, where redundancy is essential for safety reasons, the themes may focus on different means of navigation service delivery, i.e. terrestrial based, satellite based, or self-contained. Unlike the earlier interim architectures, hybrid architectures were not artificially restricted to specific regions of the trade space. Rather, each hybrid architecture – usually a fewer number than the candidate architectures - represents a rational and deliberate integration of concepts and technologies spanning the trade space. The design of each hybrid is based on the results of the earlier concept assessments and is intended to meet customer needs through the integration of concepts and technologies that can incorporate capabilities outside the assigned vector if no reasonable or rational solutions exist within the vector itself.

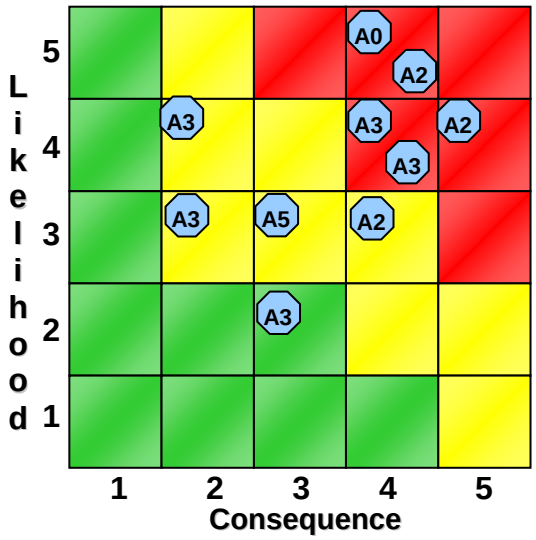


Figure 9 – "Hybrid A" Risk Profile

As features from the candidate architectures are incorporated into the hybrid architectures, the risks associated with each feature are transferred, and the earlier identification and analysis steps are updated, resulting in development of a risk likelihood (probability) template for each hybrid architecture. An example is illustrated in Figure 9.

The overall flow from concept to recommendations is illustrated in Figure 10.

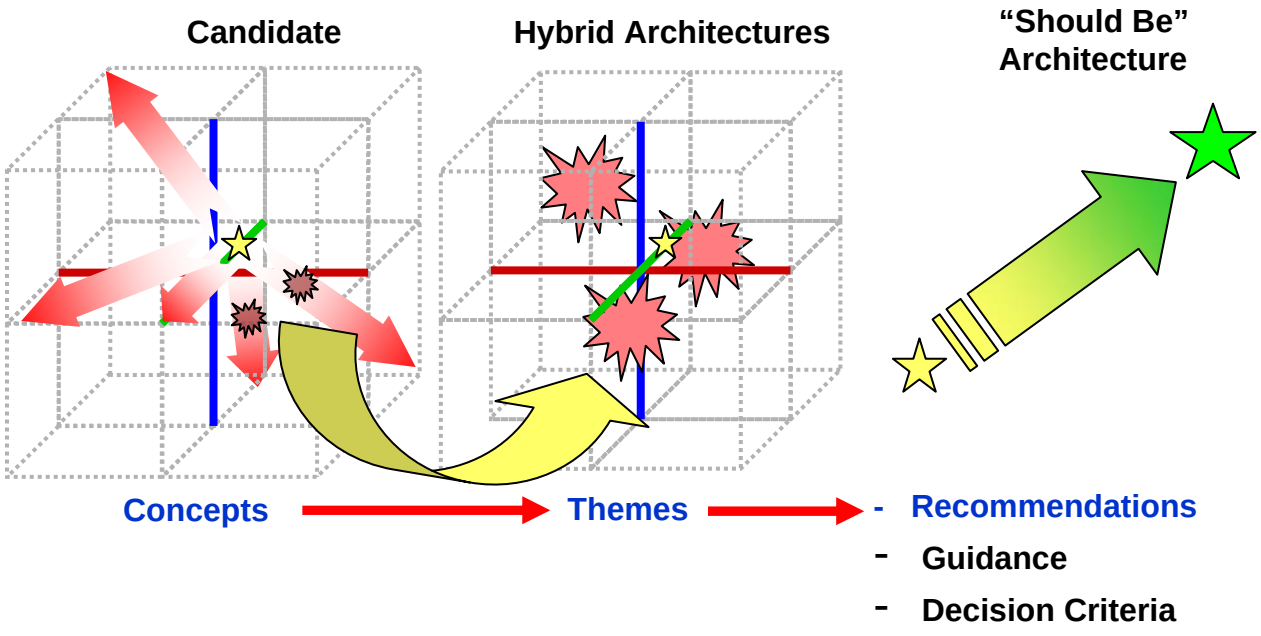


Figure 10 – The Maturation of an Architecture

Recommendations. The hybrid architecture assessment shapes the recommendations for a final functional architecture. The final recommendations and vision are based on the insights gained from the evaluation of the aspects, features, and perceived strengths and shortfalls of the hybrid architectures, rather than trying to pick a "winner" from among the hybrid architectures. As each feature (either concept or subset of a concept) are validated as contributing to the final architecture, the risks that are bound to those concept fragments are imbedded in the final outcome. Features are added or eliminated based on the risk tolerance of the stakeholders.

Transition to Implementation. Once the fundamental strategy and recommendations are formulated and validated by the stakeholders, the architectural team turns to developing planning necessary to turn the architecture into reality. The objective of risk mitigation or risk reduction efforts at this stage of the effort is to implement appropriate and cost-effective risk mitigation plans to reduce or eliminate the risks remaining. In Figure 1, a decision point (red diamond) is shown at the point that the mitigation plans are accepted, modified, or rejected. In the architectural process, this occurs as part of the decision process concerning the transition plans developed for each architectural recommendation. Implementation of the mitigation plans occurs as part of the implementation of the recommendations themselves.

Each of the residual risks (red & yellow) associated with the concepts in the final architecture are grouped with the architectural recommendation(s) that the risk has the most bearing on. Where appropriate, like risks are consolidated into a group, especially where a common set of mitigations will be effective. This approach allocates the risk mitigation to a solution subset of the architecture on behalf of the architecture as a whole. The transition plan for that related set of recommendations address the risks involved and the mitigations recommended as part of the overall transition of the architecture to implementation. This process is shown in Figure 11.

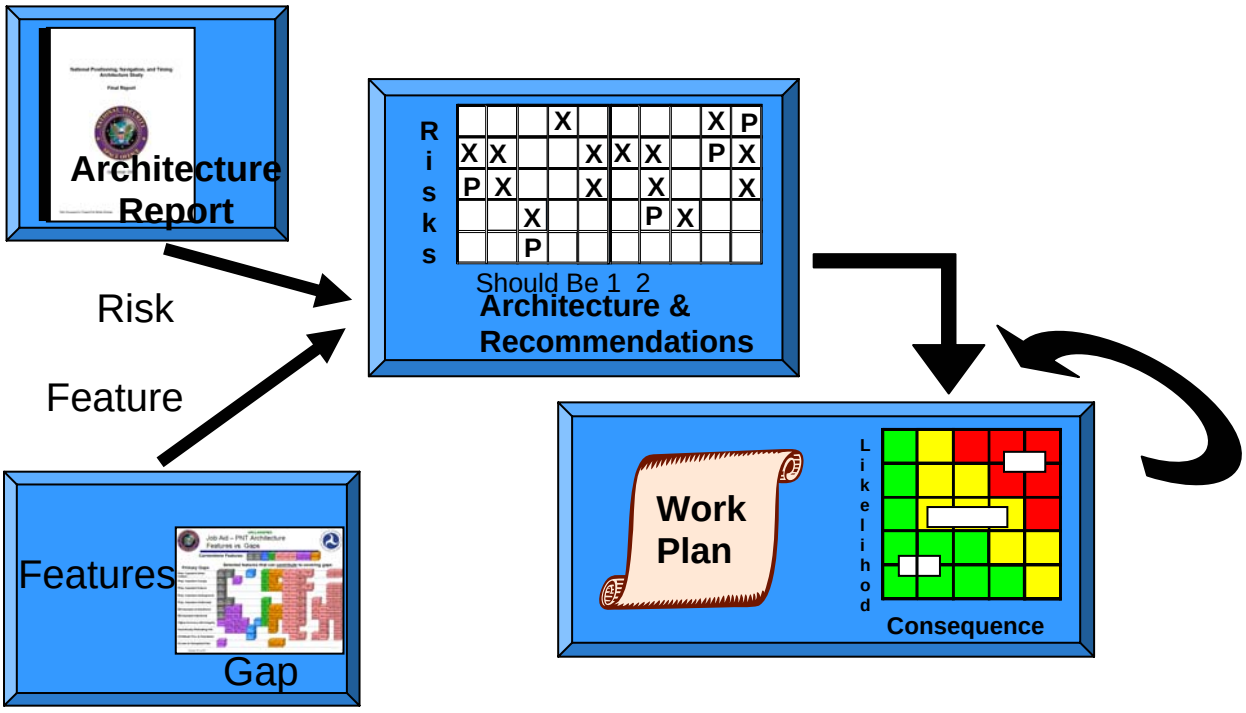


Figure 11 - Transition Planning Risk Allocation and Assessment

The recommendation set is coded in the Risk Allocation matrix (RAM) with a given aspect of the architecture coded with a “P” for primary responsibility for mitigation. The other areas of the architecture that benefit from the mitigation are coded with an “X”. Consequently, there are multiple “X”s, but only one “P” per risk. Any risks remaining after the implementation plans are developed are addressed by the architectural features specifically affected The transition and implementation focus will also shift to identifying recommendation interdependency risks and appropriate mitigations or decision points for each.

Conclusions. Inclusion of risk in the architecture development ensures that the concepts and courses of action with extreme risk are generally avoided and/or filtered out of the various architectural features generating these risks as they are identified. Alternatively, the subsequent individual hybrid architectures are designed to eliminate or mitigate such risks. Risks which remained in the "Should-Be" Architecture are considered when developing recommendations, in many cases including focused research, development, or assessment designed to mitigate such risks, vice immediate implementation of a high risk feature.

The residual risks are documented in the final architecture report, and should be considered for further mitigation during follow-on activities such as implementation planning. In the end, a functional architecture is produced that addresses stakeholder needs, while enabling a risk-informed basis for making decisions concerning the future.

Author Biography. Ken Kepchar is the Chief Systems Engineer for Integration and Information System Security within the FAA Air Traffic Organization. In this position, he is a member of the FAA Enterprise Architecture Board, and the lead instructor for System Engineering, Risk Management, Information System Security for System Engineers and Validation & Verification. Ken has over 40 years of technical experience in the aviation industry, 25 of those years in management.

Ken, has held numerous positions at the chapter and International levels of the International Council of Systems Engineering (INCOSE). He has served on the INCOSE Board of Directors and most recently as the initial Program manager and Chair of the Certification Advisory Group for the INCOSE Certified System Engineering Professional (CSEP) program.

Ken holds a B.S. (aeronautics and astronautics) from the Massachusetts Institute of Technology and an M.S. (engineering management) from the University of Missouri – Rolla. Ken is a Certified System Engineering Professional (CSEP) and a registered Certified Information System Security Professional (CISSP).