Chapter 3 – BEST PRACTICES FOR SYSTEM INTEGRATION

3.1 PROBLEMS OF SYSTEMS ENGINEERING

The Introductory chapter expresses a 'Systems Engineering Process' as a sequence of identifiable aspects, which are described below.

1) **Breaking the system down into component parts** has been done very well historically. It has produced well-defined disciplines in scientific areas such as propulsion, aerodynamics, hydrodynamics, structural design, etc. If we recall conventional aircraft design, for instance, the process was to optimize the various parts, then build multiple prototypes against a set of requirements and fly them to choose the winner.

2) **Understanding each individual part** might has been done with a good degree of success. Individual technical disciplines are quite well understood, however they require continued research progress as a function of their level of maturity.

3) **Determining how the parts interact** is not a straight forward process, and interactions are often found in flight tests and field work. One example of progressing past understanding the 'individual part' for aircraft design is the area of Multidisciplinary Optimization (MDO). It started as efforts to integrate the calculation of air loads into the structural optimization. This field is also expanding, e.g. by inclusion of control aspects. We thus have a question of how to define the interactions, how to assess the significant interactions vs. the negligible. The appropriate answer can be expected to be unique for different applications.

4) **Defining the contribution of each component to system performance** is a continually improving process. But we can ask the question of what system metric is appropriate if components are designed (optimized) to different aspects. Also, what system model is needed for any particular aspect ? What is the necessary level of fidelity?

5) **Putting the system back together** in the ideal sense would require a complete physics-based model. In the practical world, however, there are many questions to be addressed and many potential problems. How have the components been validated as being ready for system integration? One part of the preceding question is what data is experimental and what is analytical. It should not be assumed that any of the data is completely accurate, so that an explicit accounting of uncertainties is required. How have the component disciplines been coordinated during the design process? Linear superposition?

6) **The final aspect,** i.e. build it when the analysis shows that the design meets requirements, also raises many questions. What is the appropriate analysis or should it be analyses? The answer to this question may be not the same for all applications. There may be the exception for minor evolutionary upgrades to an existing system, but even that should not be taken for granted.

As a final comment, we strongly suggest that 'System Engineering' should not be applied as a sequential process, but as a continual iterative process following best practices as defined in the following section.

3.2 SYSTEMS ENGINEERING BEST PRACTICES

At the time this Task Group began, The Columbia Accident Investigation Board's (CAIB) report [Anon 2003b] had just been released. In reviewing that report, the members of this Task Group found many lessons learned in the management of high-technology endeavours which are applicable:

- Don't use prior success as an indicator of future success or as a rationale for accepting increased risk. Don't normalize deviations (where undesired, unexpected or unexplained behaviour of a component of the system is progressively accepted as normal). Anomalies should not be used as a source of engineering data to justify further operation.
- Within technical and programmatic organizations minority opinions must be sought, encouraged, even created at times for a healthy debate. Play "devil's advocate" to force issues and data into the open.
- Never stop "what-if" games. They are the heart of an effective Failure Modes and Effects Analysis (FMEA).
- Individuals must assume "ownership" and believe they are personally accountable for the success of both their part of the whole and for the whole itself. (This was one of the characteristics of the members of the F-22A Flying Qualities Working Group and is viewed as a major contributor to the success of F-22A flight control development [Harris and Black]).
- Specify component, subsystem, and system characteristics and operating environment carefully and thoroughly, test to specification(s), and fly what you've tested (and test what you fly). If deviations occur and they are outside specification and test boundaries, retest to the revised boundaries and fix anything that does not pass the new test(s).
- Successful high-technology endeavours share a characteristic of very thorough, disciplined design, test build up, and operations processes.
- Systems Engineering takes a finite amount of time and resources to do it right. Compressing schedules increases risk, sometimes dramatically.
- Use trend analysis and statistical analysis to look for warning signs of pending problems.
- In the last 15 years there has been a strong push to apply organizational structures and philosophies which have been very successful in the mass production of consumer goods to Research and Development programs and organizations. These production organizations tend to be hierarchical and can be characterized by manage-by-efficiency ("faster, better, cheaper") organizational structures and methods. Chapter 8 of the CAIB report strongly criticizes the application of such management models to high-technology experimental efforts.

The final point is worth further elaboration. One of the members of the CAIB was Brigadier General Duane Deal. Subsequent to the release of the CAIB report he authored an article delineating his own views and lessons learned as a result of his participation in the Columbia accident investigation [Deal]. (The authors of this report **strongly** recommend **any** participant – engineer, manager, or other – in research and development of advanced technology read this article.). Among his observations, General Deal highlights the temptation to become focused on *process* over *product* (emphasis in the original), and says the following about managing high-technology endeavours:

> *"A healthy pessimism is required in high-risk operations. (A) preference for a clever analogy can serve as a recipe for repeating catastrophic mistakes, whereas insistence on analysis over analogy can prevent potentially disastrous situations."*
>
> *"Although bombarded by "management by objectives"; Deming-driven, off-site quality thrusts; and "one-minute-management" techniques, leaders must ensure that the latest "organizational fad" does not negatively influence their operations. ...These principles ... work well in a manufacturing process producing 10,000 bolts a day, or at a scheduled airline where a technician may perform the same steps dozens of times per week. However, the same principles do not necessarily apply in an environment where only three to six flights are flown each year, and workers may accomplish certain processes just as infrequently. Process verification must be augmented when critical operations take place with an "eyes-on, hands-on" approach."*

"To avoid developing a focus on metrics for metrics' sake, the quantity being measured must be understandable, applicable, measurable, and the goal must be attainable. Ideally, there should exist a process that consolidates and assimilates data from multiple databases, providing a comprehensive picture of system performance, costs, malfunctions, and other trends of utility to management."

"In the 1990s, the NASA top-down mantra became "Faster, Better, Cheaper." The coffee-bar chat around the organization quickly became, "Faster, Better, Cheaper? We can deliver two of the three – which two do you want?" While the intent of the mantra was to improve efficiency and effectiveness, the result was a decrease in resources…"

"Leaders must contemplate the impact of their "vision" and its unforeseen consequences. Many must also decide whether operations should be primarily designed for efficiency or reliability. The organization and workforce must then be effectively structured to support that decision, each having a clear understanding of its role."

"Leaders must remember that what they emphasize can change an organization's stated goals and objectives. If reliability and safety are preached as "organizational bumper stickers," but leaders constantly emphasize keeping on schedule and saving money, workers will soon realize what is (really) deemed important and change accordingly."

Regarding Quality Control/Quality Assurance, "checks and balances using "healthy tensions" are vital to establish and maintain system integrity in programs from the federal government to aviation. High-risk operations dictate the need for independent checks and balances. Successful organizations must have a review process that addresses the findings and recommendations from third-party reviews and then tracks how that organization addresses those findings. To further this approach, leaders must establish and maintain a culture where a commitment to pursue problems is expected – at all levels of the program and by all of its participants."

Regarding Configuration Control, "Leaders must insist on processes that retain a historical knowledge base for complex, legacy, and long-lived systems. Configuration waivers must be limited and based on a disciplined process that adheres to configuration control, updated requirements, and hardware fixes. If workers at the lower level observe senior leaders ignoring this path, routinely waiving requirements and making exceptions to well-thought-out standing rules, they too will join the culture of their seniors and begin accepting deviations at their level – adding significant risk to the overall system. Senior leaders must also ensure the steps required to alter or waive standing rules are clearly understood."

The authors of this report assert that the Systems Engineering process as applied to the development of the flying qualities of the F/A-22 fits the criteria of healthy development outlined by Deal and the CAIB, and can be extrapolated to complete systems and to systems of systems. The key (from a technical perspective) is that a simulation model of the complete system be designated as the "truth model" of the system and be subjected to the disciplined development and configuration control process described above in this report. It should be noted that the "truth model" simulation need not include physics or thermodynamics based models at the component or subcomponent level (such as imbedding a cycle deck of a jet engine in the simulation), only that the component models within the truth model be sufficiently detailed for the purposes for which the simulation will be used, and that their operation and effects are directly traceable to the more highly-detailed component models (which is their "pedigree). Other keys displayed by the F-22 FQWG were the assumption of ownership of the aircraft and its safety and success by the members of the FQWG (already discussed) and a healthy scepticism and commitment to find and address potential problems and issues (expressed by one of the members of the FQWG as "if we are our own worst critic, we need not fear any independent review.").

3.2.1 Land Systems

Although the unstructured, outdoor terrain encountered by unmanned ground vehicles (UGV) is extremely demanding, it is also very forgiving. Under most circumstances, especially R&D situations, a UGV can simply chose to stop. Thus, the response to a system problem or error is relatively straight forward, the UGV stops and waits for external assistance. A UGV's complex yet forgiving environment stands in stark contract to a UAV's simple yet unforgiving environment. A UAV doesn't have the "stop" option, it must be under active control until it successfully lands on the ground. As a result, quality control and assurance are paramount for UAVs, but at this point in time are significantly less important for UGVs.

Historical and current UGV systems focus on sensing, representing and understanding the complex environment in which they must operate. This "obsession" with the environment means that UGV systems have not placed a significant emphasis on quality control and assurance. DARPA's second Grand Challenge clearly illustrates the current state of UGV system development. Twenty-three UGVs qualified for the race and only 5 UGVs completed the course. An analysis of the 18 unsuccessful UGVs revealed that only 3 of the failures were directly attributable to a misrepresentation of the environment. The remaining 15 failure modes ranged from mechanical failures, to electrical problems such as sensing failures, to software bugs. The teams that were successful recognized the importance reliability and quality. The race winner, Stanley, formed an independent Testing Group whose sole responsibility was testing [Thrun et al, 2006]. Second and third places where taken by vehicles from Carnegie Mellon University, and this teams development process consisted of short development cycles interleaved with periods of intensive field testing [Urmson et al]. It should also be noted that all successful teams used commercially available vehicles, which undoubtedly contributed to more reliable implementations.