Yes Virginia, You Can Build a Defect Free System, On Schedule and Within Budget.

Joe Kasser
The Anticipatory Testing Corporation
POB. 3419
Silver Spring
MD. 20918
Phone 301 593 3316
E-mail jkasser@iee.org

ABSTRACT

Today's software and systems development life cycle paradigm is characterized by large cost overruns, schedule slips, and dramatic performance deficiencies in weapon, C4I, and automated information systems. This paper describes an alternative paradigm that can produce defect free systems on schedule and within budget.

INTRODUCTION

According to the [DoD, 1995] today's software and systems development life cycle (SDLC) paradigm is characterized by big cost overruns, schedule slips, and dramatic performance deficiencies in weapon, C4I, and automated information systems.

Most people do not realize **there is an alternative** SDLC paradigm. The use of elements of this alternative paradigm enabled the design, development, production, and installation of a network of approximately 600 microprocessors controlling the solar collector section of the world's first commercial Solar Electrical Power Generating Station (SEGS-1) on schedule and within budget half way around the world from the development location. The early phases of the SDLC took place in Jerusalem, Israel, the installation was near Barstow, California. The system worked first time on initial installation with only a single Discrepancy Report (DR)[1] in spite of geographic, cultural and language difficulties. In addition, the control system was optimized for a cost savings of at least $300,000.

The alternative SDLC paradigm uses an *integrated product-process* **and management** approach. Since systems engineering techniques are used on the organization as well as on the process and the product, the paradigm is called *organizational engineering* and:

- May be used with conventional or object oriented design methodologies.
- Applies to large, and small systems.

The elements of the *organizational engineering* paradigm discussed in this paper, are:

- Partitioning the system
- Partitioning the implementation
- Proactive progress management

PARTITIONING THE SYSTEM

For any system or subsystem, its boundaries are determined by the observer for the sake of simplifying the analysis and design activities. The first level of decomposition of the system is always as shown in Figure 1. Systems may contain up to five top level subsystems as appropriate, namely, the:

- **User interface** - The data display and entry device(s) which interact with the users. The user

[1] for a bad type of cable connector.

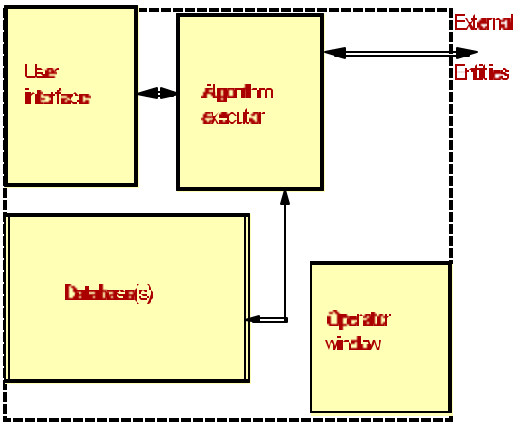

Figure 1 Top Level System Decomposition

interface is developed by a single group which ensures consistency.

- **Algorithm executor** - The top level subsystem which carries out the work the system is built to perform.
- **Database(s)** - The database components of the system.
- **Operator Window** - A window into the system. It can display all status, alarm, error and event states, and the contents of buffers. It must be designed to display data in a hierarchical manner, with the top level being a simple display of the status of the system. For example, condition:
  - *'green'*. Everything is operating according to specifications.
  - *'yellow'*. Minor failures are present, but the system is operational. For example, a failure has occurred, but the redundant component has been activated, or an interface has failed and part of the system is not operational.
  - *'red'*. The system is non operational.

  The Operator Window also serves as a major troubleshooting tool both during system commissioning and operational troubleshooting. This feature reduces the need to develop custom tools to test portions of the system, hence reducing the cost of the system.
- **External interfaces** - The interfaces to the external elements to the system.

Rules for subsystem decomposition. The rules for decomposing the major subsystems are as follows:

- **Minimize coupling and maximize the cohesion** of the functions performed by lower level subsystem elements. This approach is based on the [Ward and Mellor, 1985] Methodology and fits nicely into both object oriented and conventional design approaches.
- **Consider the operator as part of the system** - This approach allows early builds of a system to perform functions manually, and then provides automated capabilities in subsequent builds as more is learned about the system's behavior. It also allows systems to be coupled in a well-defined manner. For example, one system may act as "the operator" for a second system.
- **Self-regulating subsystems** - Subsystems are designed to perform their tasks in a self regulating manner. The rules for (minimizing) coupling and (maximizing) cohesion must be observed. The subsystem transmits status information about itself, and receives command instructions from other subsystems. This approach, shown in Figure 2 has many variations. For example:
  - **Spacecraft or missile control**. In an early implementation of a family of spacecraft for communications or observations, System A is on the spacecraft and System B is on the ground. System B performs complex control and monitoring functions that System A

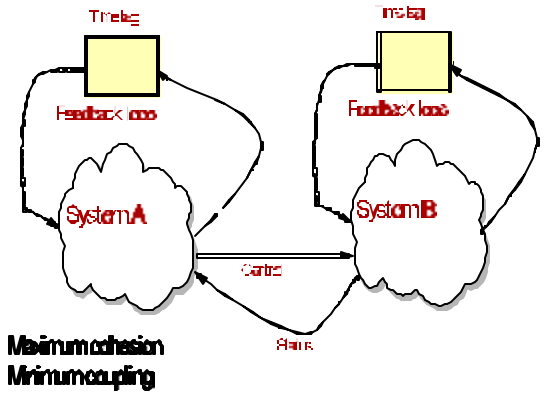

Figure 2 Self Regulating Systems

cannot. Some System B functions may be even be performed by human operators and analysts. As technology matures, or new technology becomes available, some System B functions are migrated into System A. The advantages of this approach include:

- Most of the requirements for later generations are known, algorithms have been developed and tested code and requirements may be reused for replacement and later generation spacecraft.
- Faster control responses
- In case of an onboard malfunction of the migrated functions, System B is still available on the ground to take over.

- **SEGS 1 Sun tracking**. Each of the SEGS 1 collectors had to be positioned within ±0.1 degree of the Sun. The sun sensor which detected when the array was pointed at the Sun, was mounted on the collector. There was no specification for the vibration of the collector due to wind or internal mechanical causes Each sensor contained a pair of photo diodes and a shield. There was no specification on the sun-sensor other than an uncalibrated output curve showing relative change of output with sun angle as the Sun passed across a typical prototype sensor. The computed pointing angle for each collector was a function of the mounting accuracy of the sun sensor, the latitude and longitude of the site and the alignment of the collector array with respect to North. In addition, there was no specification for the accuracy of the measurement of these parameters. The principle of self regulation was applied to develop a successful positioning algorithm that allowed for large tolerances on all these parameters.

- **Railroad buffers for signal passing** - This is a key element to the paradigm. All signals are passed between processes via buffers at both ends of the interface as shown in Figure 3. Modules are not allowed to build and transmit messages on the fly, or react to messages as they are received. The term 'railroad buffers' is used because the interface area of a system may look like a freight yard at a railroad station. This element allows modules to be tested in both a static (standalone) and a dynamic manner. The interface is tested by placing known data in a transmitter buffer and ensuring the data appearing in the corresponding receiver buffer is correct after the necessary event which initiates the transfer takes place. The modules are tested by placing data in the receiver buffer, and initiating the processing task. The data in the output buffer or the state of the module is then checked to see it meets the specifications for the processing task. This element has much in common with client-server techniques, but may cause a small loss in performance. These buffers may also be considered as the software equivalent of hardware test points.

PARTITIONING THE IMPLEMENTATION

The implementation of the system takes place according to the following approach:

- Design and implement the structure of the system
- Flesh out in subsequent builds
- Build a little, test a lot
- Anticipate changes
- Budget tolerant methodology
- Cataract approach
- Prevent defects

- **Design and implement the structure of the system** The initial Build provides the structure of the

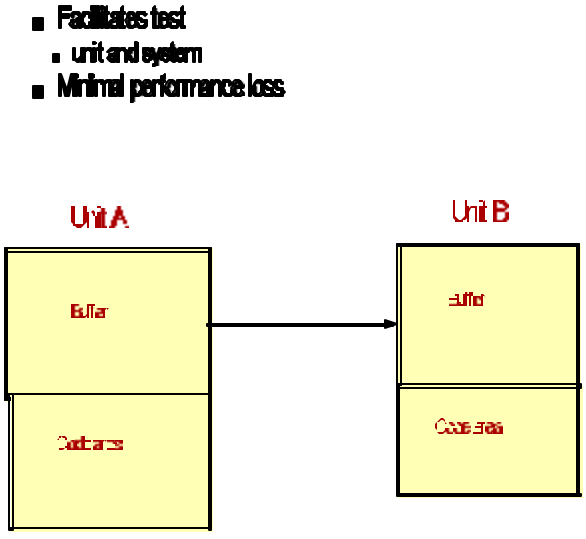

Figure 3 Railroad Buffers for Signal Passing

system, the user interface and the operator window.

C

Flesh out in subsequent builds - Once the structure is in place, elements of the subsystems may be added in an incremental manner. The actions of the system may be observed via the user interfaces, and the operation verified by means of the operator's window. The subsystems builds must be synchronized so that the user interface and operator window subsystems are updated in advance of the implementation of the algorithms accessed by the interfaces and operator window.

C **Build a little, test a lot** - With a working user interface, and operator window, elements of the system may be built and tested in an incremental manner using all the best practices. Conventional SDLC Builds take a minimum of six months. This approach allows for shorter Builds, of the order of weeks or even days. Software systems developers can ship sample copies to selected users for comments well before the release of the complete product.

C **Anticpate changes** - Changes are continuous for various reasons which include changes:

  C In the mission definition.
  C Due to user reaction to early builds.
  C Due to changes in the project budget.

  Since changes are common to all projects, the SDLC must incorporate a change tolerant methodology to be successful. *Success is defined as a completed project, which meets its requirement, and is completed on schedule and within budget.*

C **Budget tolerant methodology -** In today's systems engineering environment, budgets are decreasing while needs are remaining constant or even increasing. Consequently, systems must be designed so that in the event of budget reductions, there is no need to cancel the project and restart the development of a system with lower capability [Denzler, Kasser, 1995]. The budget-tolerant system development methodology is based on the traditional waterfall SDLC model with enhancements that require the consideration of the costs and the importance of the requirements as necessary elements in the analysis and design processes. The methodology consists of seven steps:

1. Determine the feasibility of a requirement
2. Develop a complete set of requirements
3. Prioritize the requirements
4. Cost each requirement
5. Establish a baseline
6. Use the cataract approach to build planning
7. Use effective change management techniques

C **Cataract approach -** The cataract approach [Kasser, 1995] plans the system implementation in a series of Builds wherein each Build contains a full waterfall or mini SDLC. *This approach allows changes to occur under configuration control*. The cataract approach to Build planning may be likened to a rapid prototyping scenario in which the requirements for each Build are frozen at the start of the Build. This approach, however, is more than just grouping requirements in some logical sequence and charging ahead. Build plans must be optimized on the product, process, and organization dimensions as follows:

  C Use the waterfall approach for each Build. This tried-and-true approach works over a short timeframe.
  C Implement the highest priority requirements in the earlier Builds. Then, if budget cuts occur during the implementation phase, the lower priority requirements are the ones that can readily be eliminated because they were to be implemented last.
  C Make use of the fact that, typically, 20 percent of the application will deliver 80 percent of the capability [Arthur, 1992] by providing that 20 percent in the early Builds.
  C Produce each Build with some extra degree of functionality that it can be used by the user (customer) in a productive manner. This follows the rule of designing the system in a structured manner and performing a piecemeal implementation.
  C Allow a factor for the element of change
  C Optimize the amount of functionality in a Build (features versus development time).

- Minimize the cost of producing the Build. Balance the number of personnel available to implement the build (development, test, and systems engineers) over the SDLC to minimize staffing problems during the SDLC.

- **Prevent defects** - Traditional Quality Assurance and Testing functions are independent from the Development effort and act after the fact. Consequently, errors are first made and then corrected. This means the elements in the Work Breakdown Structure are planned and budgeted as one time efforts, yet are in fact performed twice, resulting in overruns and delays. The anticipatory testing approach [Kasser, 1995] combines prevention with in-process testing in a synergistic manner to eliminate defects in two ways, namely, by:

  - **Testing** - The earlier the testing can be performed in the SDLC, the greater the reduction in the penalty costs of not doing it right the first time, so do the testing at well established checkpoints in the SDLC. These check points include:
    - Concept reviews.
    - Implementation (Management) Plans.
    - Requirements reviews.
    - Design reviews.
    - Code walkthroughs.
    - Code inspections.
    - Test Plan reviews.
    - Test Procedure reviews.

  - **Prevention** - According to [Crosby, 1981] Prevention is planned anticipation and includes:
    - Sensitization to probable defects (training).
    - Improving the process
    - Risk management

PROACTIVE PROGRESS MANAGEMENT

Many of the measurements made in current projects enable suppliers to improve their processes and products. These may be used for proactive progress management in several ways, including:

- **Improvement of the Quality Index** - These measurements may be used to lower the cost of doing work by improving the *Quality-index* of the organization [Kasser, 1996] which is a three dimensional measure of the:

  - Effectiveness of the production process.

  - Degree of conformance of the product to its requirements.
  - Effectiveness of the organization in which the process takes place.

- **Use the categorized requirements in process chart** - The budget tolerant methodology categorized requirements by cost (to implement) and priority. Tracking the implementation of the categorized requirements led to a measurement approach called *categorized requirements in process* (CRIP) which

  - has **the potential of providing a measurement of completeness of the product at any of the milestones in the SDLC**.
  - Categorizes the requirements, then quantifies each category into ranges, and observes changes in the state of the requirements at the SDLC reporting milestones

The CRIP approach has the following advantages, it:

- Maybe used at any level of system decomposition.
- Provides a simple way to show progress or the lack of it, at any reporting milestone. Just compare the numbers and ask for an explanation of the variances.
- Provides a window into the project for top management (buyer and supplier) to monitor progress.
- Identifies some management and technical problems as they occur, allowing proactive risk containment techniques.
- May be built into requirements management, and other computerized project and design management tools.
- May be built into Government contracts via the SOW. Here falsifying entries in the CRIP chart to show progress is fraud.

SUMMARY

Defect free systems can be built on schedule and within budget. However, to do so requires integrating the product, process and organization dimensions. In addition, this integrated state is not readily achieved in

today's systems and software development organizations. So Virgina, when you follow the main elements of the *organizational engineering* approach to providing defect free systems on schedule and within budget described in this paper, remember to sweeten everything with a KISS (Keep it simple stupid).

REFERENCES

Crosby, P.B., *The Art of Getting Your Own Sweet Way*, Second Edition, McGraw-Hill Book Company, 1981, p 131.

Department of Defense, *The Program Manager's Guide to Software Acquisition Best Practices*, Version 1.0, July 1995.

Arthur, L.J., *Rapid Evolutionary Development*. John Wiley & Sons, Inc., 1992.

Denzler, D.W.R., Kasser, J.E., "Designing Budget Tolerant Systems", *The INCOSE 5th International Symposium*, St. Louis, MO, 1995.

Kasser, J.E, *Applying Total Quality Management to Systems Engineering*, Artech House, 1995.

Kasser, J.E., "There's No Place For Managers in a Quality Organization", *The 9th Annual Conference on Federal Quality*, Washington DC., 1996.

Ward, P.T., Mellor, S.J., *Structured Development for Real-Time Systems*, Yourdon Press Computing Series, 1985.

BIOGRAPHY

Joe Kasser earned his doctoral degree in systems engineering in 1997. He is a recipient of NASA's Manned Space Flight Awareness (Silver Snoopy) Award for quality and technical excellence. He is also an Institute of Certified Professional Manager's (ICPM's) Certified Manager and a recipient of the ICPM's 1993 Distinguished Service Award. He is the author of *Applying Total Quality Management to Systems Engineering* published by Artech House. His paper "Systems Engineering - Myth or Reality" won the Systems Engineering Management Outstanding Paper Presentation Award at last year's symposium.