Software Process Assurance for Complex Electronics

Richard A. Plastow
Science Applications International Corporation
NASA Glenn Research Center

July 24, 2007

Complex Electronics (CE) are now programmed to perform tasks that were previously handled in software, such as communication protocols. Many of the methods used to develop software bare a close resemblance to CE development. For instance, Field Programmable Gate Arrays (FPGAs) can have over a million logic gates while system-on-chip (SOC) devices can combine a microprocessor, input and output channels, and sometimes an FPGA for programmability. With this increased intricacy, the possibility of “software-like” bugs such as incorrect design, logic, and unexpected interactions within the logic is great.

Since CE devices are obscuring the hardware/software boundary, we propose that mature software methodologies may be utilized with slight modifications in the development of these devices. Software Process Assurance for Complex Electronics (SPACE) is a research project that looks at using standardized S/W Assurance/Engineering practices to provide an assurance framework for development activities. Tools such as checklists, best practices and techniques can be used to detect missing requirements and “bugs” earlier in the development cycle creating a development process for CE that will be more easily maintained, consistent and configurable based on the device used.
Software Process Assurance for Complex Electronics (SPACE)

Richard A. Plastow
Science Applications International Corporation
NASA Glenn Research Center

July 24, 2007
The Quandary

Complex Electronics (CE) devices can have over one million gates and even a built-in microprocessor. These devices are replacing conventional software in many critical applications. How do we assure quality on these devices?
How the Design Process For Complex Electronics should flow
Planning is Where to Start

Project Design includes Complex Electronics

Determine
- Simple/Complex
- Criticality

Engineering

CE Development Plan
- Management (schedule, resources, responsibilities)
- Design Methodology
- Language
- Toolset
- C/C++

Supporting Processes
- Configuration Mgmt.
- Problem Reporting

Verification/Validation Plan
- Verification Methods
- Testing Strategy
- Validation Methods

Assurance

Review and Approve

CE Assurance Plan
- Management (schedule, resources, responsibilities)
- Reviews (documents, code)
- Audits (process)
- Analyses

Review and Approve

Approved Plans
Simple or Complex?

◆ The Federal Aviation Administration (FAA) provides a definition in DO-254, “Design Assurance Guidance for Airborne Electronic Hardware” document. It states “A hardware item is identified as simple only if a comprehensive combination of deterministic tests and analyses appropriate to the design assurance level can ensure correct functional performance under all foreseeable operating conditions with no anomalous behavior. When an item cannot be classified as simple, it should be classified as complex. An item constructed entirely from simple items may itself be complex.”

◆ Firmware is not CE. The most common definition is found in IEEE 610.12-1990: “The combination of hardware device and computer instructions and data that reside as read-only software on that device.”
What is the Devices Criticality?

<table>
<thead>
<tr>
<th>Criticality Classification</th>
<th>Criteria</th>
</tr>
</thead>
</table>
| High                      | 1. The complex electronics executes safety-critical functions  
                           | 2. The complex electronics executes mission-critical functions and is a single point of failure  
                           | 3. The design is expected to be highly complex  
                           | 4. The design is expected to have significant risk due to one or more of these factors:  
                           |   i. Unstable requirements  
                           |   ii. Technical concerns with the chosen technology, such as power consumption, design size for the chip, timing, packaging, or operating frequency  
                           |   iii. Highly innovative and untried design approach  
                           |   iv. Highly aggressive schedule  
                           |   v. Inexperience of the design team |
| Moderate                  | 1. The complex electronics executes mission-critical functions but there is redundancy in the system  
                           | 2. The design is expected to be moderately complex  
                           | 3. The design is expected to have moderate risk due to one or more of these factors:  
                           |   i. Some requirements undefined or unstable  
                           |   ii. Somewhat innovative and untried design approach  
                           |   iii. Aggressive schedule  
                           |   iv. Design team contains some inexperienced members |
| Low                       | The complex electronics is classified as Low if it does not fall into either of the above categories |
How do You Start the Process?

- Create an Assurance Plan for your device
  - Can be stand alone or part of the larger assurance plan
  - Plan is based on criticality of device(s)
  - Get concurrence with the plan
  - One plan can cover all devices needed
# Assurance Planning is Very Important

## Assurance Planning Document

<table>
<thead>
<tr>
<th>ID</th>
<th>Process Step</th>
<th>Completion Date</th>
<th>QA</th>
</tr>
</thead>
<tbody>
<tr>
<td>1</td>
<td><strong>Entrance Criteria are met.</strong></td>
<td></td>
<td></td>
</tr>
<tr>
<td>2</td>
<td>Concur with complex electronics criticality classification (high, moderate, or low). Include in the CEAP (below)</td>
<td></td>
<td></td>
</tr>
<tr>
<td>3</td>
<td>Generate tailored Complex Electronics Assurance Plan (CEAP). This includes steps 4 through 14 below.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>4</td>
<td>Specify purpose and scope of plan.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>5</td>
<td>Determine Applicable and Reference standards and documents.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>6</td>
<td>Define management of the assurance activities, including organization structure, roles and responsibilities, resources, schedule, reporting.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>7</td>
<td>Identify training and tools required for the assurance tasks.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>8</td>
<td>Specify tasks for Requirements phase, including reviews, audits, and analyses.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Specify criteria and tasks for acceptance of complex electronics.</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Exit Criteria are met.</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Supporting Processes

- Controlling and monitoring the process used is very important.
  - Configuration Management
  - Audits
  - Selecting the development process
  - Problem reporting / monitoring
  - Risk Management
  - Ad Hoc is NOT a process!
## Involve the Correct People

<table>
<thead>
<tr>
<th>Role</th>
<th>Responsibility</th>
</tr>
</thead>
</table>
| Systems Engineer                    | - Define the system requirements  
                                 | - Decompose system requirements down to sub-system level  
                                 | - Define system-level testing                                                 |
| Electronics Designer                | - Derive requirements for the board or chip level  
                                 | - Design electronics to meet the requirements, using good engineering practices  
                                 | - Implement the design in hardware  
                                 | - Test the hardware; Implement changes                                        |
| System Safety                       | - Identify if complex electronics can cause a hazard or are part of a hazard control  
                                 | - Ensure that design errors in complex electronics are considered as a failure mode |
| CE Process Assurance                | - Assess entrance and exit criteria for each life cycle phase  
                                 | - Ensure traceability of the requirements through all levels of development  
                                 | - Analyze the products produced (documents, designs, etc.) against the requirements and the output of the previous phase  
                                 | - Perform white box analysis on CE designs and tests                          |
Requirements

The first step in any design process should be to define and document the requirements and constraints under which the CE must operate. This allows you to think through the issues and document any design decisions and trade-offs.

Complex Electronics design is often started based on the engineers knowledge of the system, not defined requirements.

Requirements Reviews
- Clear
- Concise
- Confirmable
- Traceable

Interface Control Document verifications

Signals List
# Requirements Review Checklist Snippet

<table>
<thead>
<tr>
<th>ID</th>
<th>Topic</th>
<th>Criteria</th>
<th>Yes/No/NA</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>General</td>
<td>Are the overall system configurations and operating modes defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>11</td>
<td>Interfaces</td>
<td>Is the data size and bit order defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>12</td>
<td>Signals</td>
<td>For each input signal, is the range of valid data defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>13</td>
<td>Signals</td>
<td>For each output signal, is the range of valid data defined? Is a typical value defined?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>20</td>
<td>Initial Conditions</td>
<td>During power-up or reset, do any lines or signals float?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Error Handling</td>
<td>Is the behavior of the CE in response to an external failure or fault specified?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>28</td>
<td>Timing</td>
<td>Has the timing of critical signals been defined?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Traceability Analysis

- Interface Definition
- System and Sub-system Requirements
- Safety Analyses

CE Requirements

CE Design (Model)

Netlist

Test Bench

Device Verifications

Requirements Verification Test Procedures
Design

One major difference between CE and software is the aspect of timing and concurrency.

- Design reviews are important.
- Independent engineer should review the design
- Confirm the design supports the requirements
- Use a coding standard
- Have and follow Best Practices
Fault Tree Analysis

Count Failure

OR Condition

Output Driver Failure

Logic Failure

OR Condition

Count Carry Failure

Adder Routine Failure
Although HDL is not true code, it shares many of the same features and attributes of software. Differences include:

- During synthesis (compile), the design is mapped to the logic gates of the device.
- The placement of the logic blocks within the chip, and the routing between blocks, are some of the processes that occur during implementation (link).
Ease of Coding

- Coding Standards, Code Reviews and Best Practices work well on HDLs. They allow:
  - Readability
    - Standard Signal names
    - Names do not change across boundaries
    - Common register names
  - Maintainability
  - Common naming conventions
  - Code reviews
  - Etc…..
library ieee;
USE ieee.std_logic_1164.all;
ENTITY reg8 IS PORT(
  clk, we: IN std_logic;
  rdata: IN std_logic_vector (7 DOWNTO 0);
  Asel, Bsel: IN std_logic_vector (1 DOWNTO 0);
  Acut, Bout: OUT std_logic_vector (7 DOWNTO 0) );
END reg8;
ARCHITECTURE one OF reg8 IS
BEGIN
  first: PROCESS (clk, we, rdata, Asel, Bsel)
  TYPE reg_array IS ARRAY(0 TO 3) OF std_logic_vector(7 DOWNTO 0);
  VARIABLE reg: reg_array(7 DOWNTO 0);
  BEGIN
    IF clk'EVENT AND clk='0' THEN
      IF (we='1') THEN
        CASE Asel IS
          WHEN "00" => reg(0):=rdata;
          WHEN "01" => reg(1):=rdata;
          WHEN "10" => reg(2):=rdata;
          WHEN OTHERS => reg(3):=rdata;
        END CASE;
      ELSE
        CASE Asel IS
          WHEN "00" => Acut<=reg(0);
          WHEN "01" => Acut<=reg(1);
          WHEN "10" => Acut<=reg(2);
          WHEN OTHERS => Acut<=reg(3);
        END CASE;
        CASE Bsel IS
          WHEN "00" => Bout<=reg(0);
          WHEN "01" => Bout<=reg(1);
          WHEN "10" => Bout<=reg(2);
          WHEN OTHERS => Bout<=reg(3);
        END CASE;
      END IF;
    END IF;
  END PROCESS first;
END one;
# Example of Code Review Best Practices

<table>
<thead>
<tr>
<th>ID</th>
<th>Topic</th>
<th>Criteria</th>
<th>Yes/No/NA</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>General</td>
<td>All states in a state machine are defined or invalid states are returned to a known state</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Clocks</td>
<td>Do not generate the clock using combinational logic</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Signals</td>
<td>Names shall be self-explanatory</td>
<td></td>
<td></td>
</tr>
<tr>
<td>34</td>
<td>Reset</td>
<td>Provides an Asynchronous reset line</td>
<td></td>
<td></td>
</tr>
<tr>
<td>36</td>
<td>Interfaces</td>
<td>All asynchronous inputs are first synchronized before use</td>
<td></td>
<td></td>
</tr>
<tr>
<td>39</td>
<td>Functions</td>
<td>The sensitivity list contains only the signals that should cause the process to be executed</td>
<td></td>
<td></td>
</tr>
<tr>
<td>41</td>
<td>Other</td>
<td>Are unused functions within the IP cores identified? Is the accidental execution of these functions prevented?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Test

While complex electronics use test benches and timing models, the idea of a well defined suite of test cases is common in both disciplines. This includes test plans, fault injection and error handling testing and verification.
Test Methodologies

- Best Practices
- Test Plans
  - Tracing to requirements
  - Feasible
  - Cover more than just success
  - Fault Injection
  - Test Verification
- Problem Trend Analysis / Tracking
# Test Plan Review Checklist

<table>
<thead>
<tr>
<th>ID</th>
<th>Topic</th>
<th>Criteria</th>
<th>Yes/No/NA</th>
<th>Comment</th>
</tr>
</thead>
<tbody>
<tr>
<td>4</td>
<td>General</td>
<td>Is the functionality of the complex electronics (CE) in off-nominal mode being tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>14</td>
<td>Interfaces</td>
<td>Interfaces with COTS IP modules tested</td>
<td></td>
<td></td>
</tr>
<tr>
<td>17</td>
<td>Signals</td>
<td>For each input signal, is the range of valid data tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>25</td>
<td>Initial Conditions</td>
<td>Is the state of programmable memory elements upon power-up and after a reset tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>27</td>
<td>Error Handling</td>
<td>Have all expected errors or faults been tested to verify they are handled correctly?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>30</td>
<td>Timing</td>
<td>Has the timing of critical signals been tested?</td>
<td></td>
<td></td>
</tr>
<tr>
<td>32</td>
<td>Power/Electrical</td>
<td>Is the maximum allowable power and current to the CE being verified?</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>
Reality Check

- Many assurance engineers, regardless of their specialty, have little understanding of the complexities of these devices. Any review done will only be to the level of knowledge of the assurance engineer.

  - Three courses have been developed
    - Introduction to CE
    - CE Life Cycle
    - Assurance of CE devices

- Techniques and checklists were created to ensure quality.
  - Not all techniques/checklists used on every part.
  - Dependent on criticality and project direction.
Process Flow Example

Software Design Certification Phase  Hardware Certification Phase

Software Quality to Hardware Quality Transition

Bi-directional Requirements traceability - Software Quality, Safety and Reliability Components Testing - Hardware Quality
TPS / Test Plan / Test Process review - Software Quality, Safety and Reliability System Integration Testing - Hardware Quality

Richard A. Plastow (SAIC)
Sr. Software Assurance Engineer
How Complex Electronics Fits into Review Cycles

CE Design Process Flow

SRR  PDR  CDR  TRR  SAR

CERP → CEDP → CEDDP → IMPL → V&V
Techniques

- Change Impact Analysis
- Decision Tables/Trees
- Design Evaluation
- Design Review
- Failure Mode and Effect Analysis
- Fault Tree Analysis
- Function and Physical Configuration Audits
- Interface Analysis
- Requirements Evaluation
- Requirements Review
- Risk Analysis
- Traceability Analysis
Impact Analysis Defines

- Rational for Change
- Effects on Internal Interfaces
- Effects on External Interfaces
- Effects on Hazards
- Effects on Operations
- Potential for introducing new bugs
- Impact of Change (Minor/Major and why)
- Testing/Verifications needed
- Things to Consider
Checklists

- Planning Phase
- Requirements Phase
- Preliminary Design Phase
- Detailed Design Phase
- Implementation Phase
- Testing Phase
- Operations Phase
- **Assurance Planning**
- **Modifications or Upgrades**
- **Audits** (Functional Configuration, Physical Configuration and In-Process)
- **Best Practices** (Code Review)
- **Testing** (Document Review)
Requirements Phase Process Checklist

- Overview
- Entrance Criteria
- Responsible Personnel
- Process Step – Lists Analysis to use/update, documentation (to create, update, etc.), supporting processes needed
- Exit Criteria
- Documentation Status
Conclusion

- Thanks to the NASA Software Assurance Research Program which funded this Research

- Contact Information
  - Richard Plastow
  - 21000 Brookpark Road, MS 50-4
  - Cleveland, OH 44135
  - Richard.A.Plastow@nasa.gov
  - (216) 433-3431