Software Quality Assurance for Embedded Systems

Rajiv Bhargava
Associate Director (SQA), NPCIL

Presentation on 29 October 2009 at SACET-09, VECC, Kolkata

Embedded Systems

- Electronic programmable sub-systems functionally integrated in a larger system
- May not be apparent to the user
- Should be safe, reliable, self-checking, low / no maintenance

Embedded Systems - Examples

- Aviation – flight control
- Automobiles – suspension, braking, steering
- Railways - signaling
- Medical – diagnostic, therapeutic
- Defense – control & guidance
- NPP – protection & control

Safety Classification

Railway Control	EN50128(*)	SIL 4 to SIL0
Automobiles	MISRA (*)	SIL 4 to SIL0
Aviation (civil)	RTCA-DO 178-B	Cat A to Cat E
Aerospace	ESA	None
Medical-PEMS	IEC 601-1-4	Catastrophic/ critical/ marginal/ negligible
Defense	DoD2187/DoD882B	Cat I to cat V
Nuclear	IEC 1226	IA / IB/ IC

Life Cycle Processes

- Development of requirements
- Allocation of requirements
- Realization of System
- Development process
- Support Processes
  - Planning
  - QA (HQA/SQA)
  - Configuration Management
  - Verification and Validation

Quality Objectives

- Completeness
- Correctness
- Safety
- Reliability
- Operability
- Maintainability
- Upgradability

The CBS Life Cycle

- Requirements Definition
- Procurement/Development
- Deployment

Types of CBS

- Custom Built
- Commercial Off The Shelf (COTS)
- Pre-Developed Systems

Verification:

The process of determining whether or not the product of each phase of Computer based System (CBS) development process fulfils all the requirements imposed by the previous phase (IEC 880)

Validation:

The test and evaluation of the integrated Computer based System (hardware and software) to ensure compliance with the functional, performance and interface requirements (IEC 880).

Independent V&V:

V&V carried out by an Independent agency.

Why IV&V?

- Ensure dependability of CBSs
  - Completeness (Functionality/Performance)
  - Freedom from defects
  - Robustness
  - Safety
  - Reliability
  - Operability
  - Maintainability
- Provide support for Safety Case (as necessary)

Role of IV&V in NPCIL

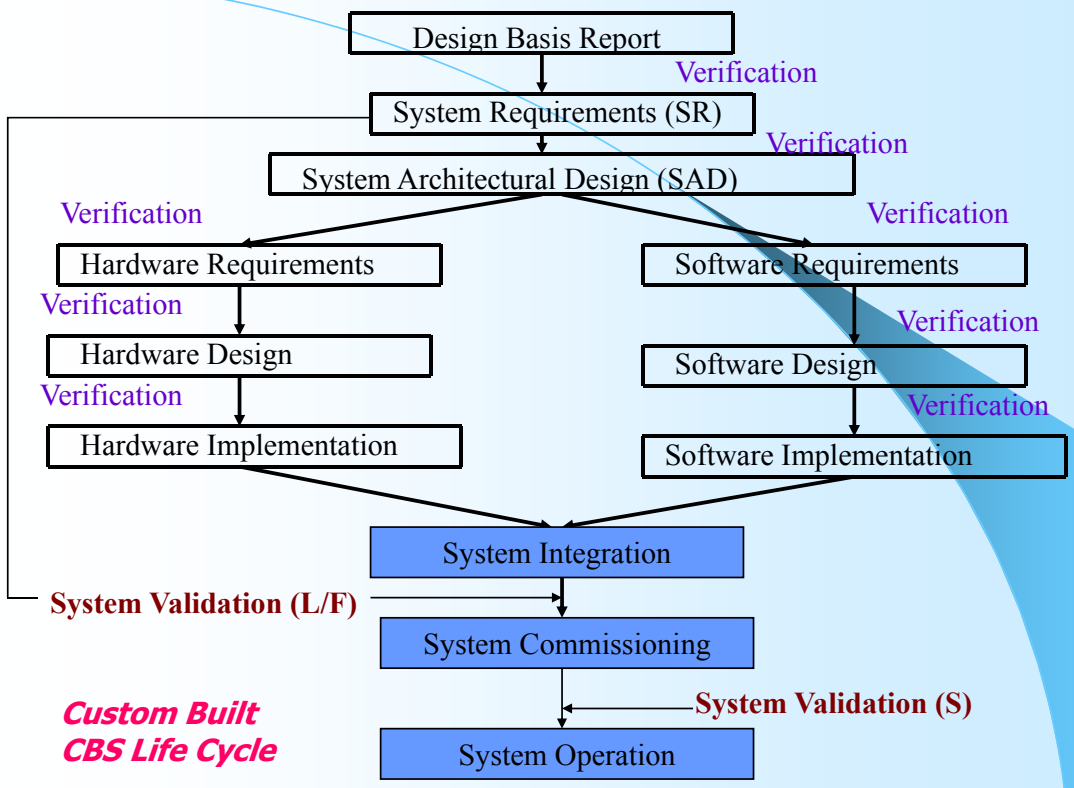
- NPCIL's internal process
- Applicable to CBSs and critical software
- Initially applied to safety and safety related systems for new projects
- Being applied to replacement systems
- Being used for assessment of CBSs in older plants during periodic safety review
- Specific IV&V reports used as part of safety case submissions to AERB for regulatory clearances
- IV&V procedures being developed for critical software, initial applications in OSPI, DMS and CFD software
- Only IV&V for Custom-Built CBSs being discussed here

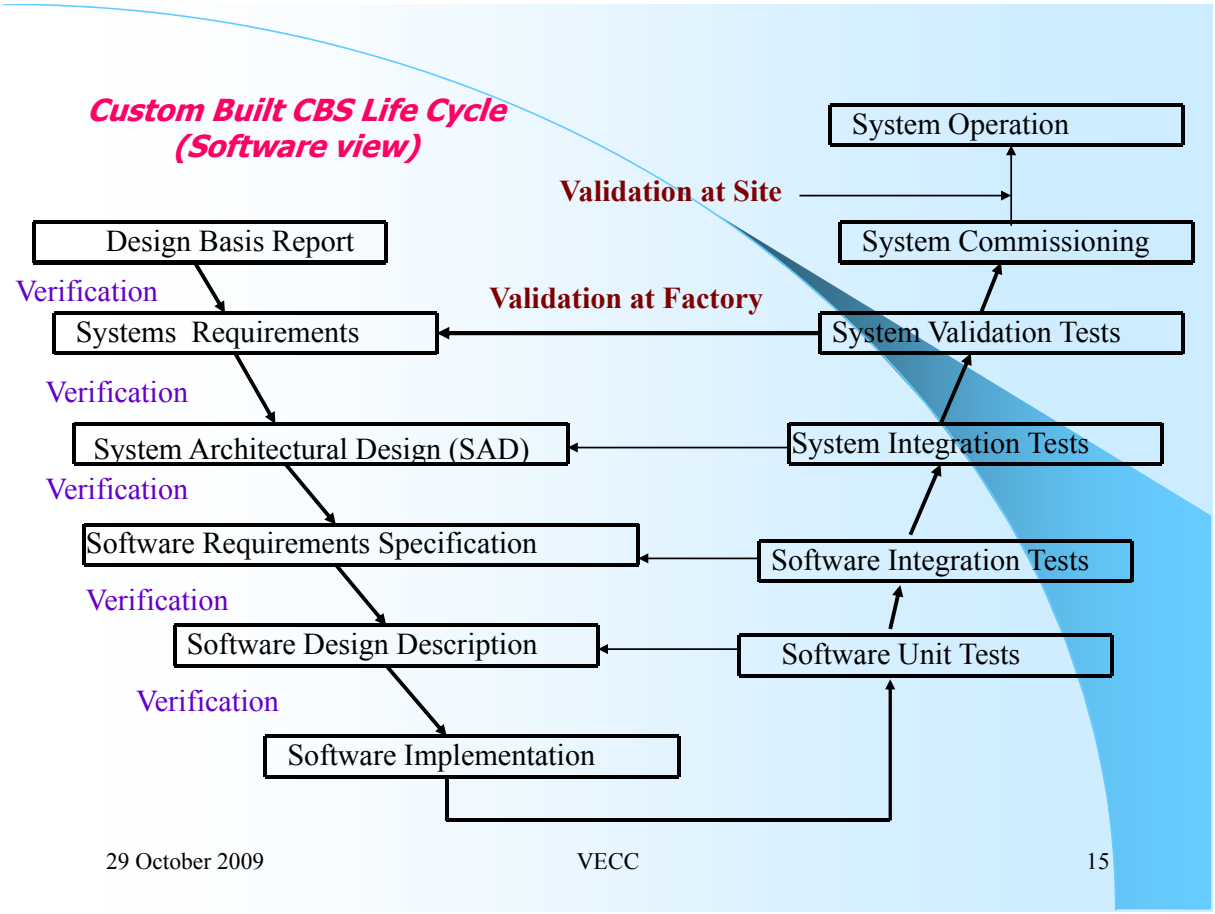
The IV&V Process for CBSs

- Different procedures for
  - Custom-Built Systems
  - COTS systems
  - Pre-Developed Systems (PDS)
- Includes verification of design documents starting from System Requirements to User Documentation and review of test reports at various levels of integration
- Includes multi-stage validation
- Envisaged as concurrent activity with design, development, manufacture and deployment
- AERB-SG-D-25 compliant, accepted by AERB

Projects/Stations covered till now

- TAPS-3&4 – All systems
- KG-3&4/RAPP-5&6 – Safety related systems
- KG-1&2/RAPS-3&4 – SR systems
- KKNPP-1&2 – SR systems
- TAPS-1&2 EMTR
- KAPS-1&2 EMTR
- RAPS-3 COIS
- NAPS- three systems





Plans

- Project Management Plan (PMP)
- System Development Plan (SDP)
- Configuration Management Plan (CMP)
- Hardware Quality Assurance Plan (HQAP)
- Software Quality Assurance Plan (SQAP)
- Hardware Verification & Validation Plan (HVVP)
- Software Verification & Validation Plan (SVVP)

Total: 7 documents on plans

Design Documents

- Design Basis Report (DBR) / Statement of Purpose (SOP)
- System Requirements (SR)
- System Design Guidelines (SDG)
- System Architectural Design (SAD)
- System Integration and Test Procedure (SysITP)
- System Validation Procedure (SVP)
- Hardware Requirements Specification (HRS)
- Hardware Design Description (HDD)
- Hardware Integration and Test Procedure (HITP)
- Software Requirements Specification (SRS)
- Software Design Description (SDD)
- Software Integration and Test Procedure (SITP)
- Programming Guidelines (PG)
- Software Implementation (Source and Object Code)
- User Documentation (UD)
- System Build (SB)

Total: 16 documents on design

Reports

- Hardware Unit Test Reports (HUTR)
- Hardware Integration & Test Report (HITR)
- Software Unit Test Reports (SUTR)
- Software Integration & Test Report (SITR)
- System Integration & Test Report (SysITR)
- System Safety Analysis Report (SSAR) (IA/IB systems only)
- Hardware Reliability Analysis (HRA) (IA/IB systems only)

Total: 7 (or 5) documents on reports

The Review Procedure

- ✓ Design Basis Report (DBR) (or SOP) is baseline document
- ✓ Consists of following review stages:

- Requirements
- System Architecture
- Hardware/Software Specification
- Hardware/Software Implementation
- System Integration
- System Validation

✓ The plans, guidelines, reports, System Build and User Documentation are reviewed for consistency and completeness.

✓ All other documents are reviewed, in addition, for traceability and various traits.

✓ The reviews for design documents are carried out as per checklists.

Requirements Review

- ✓ Documents submitted:
- Design Basis Report (DBR)
- System Requirements (SR) (with Traceability Matrix)

- ✓ Activity:

The major traits examined for SR are:

- System's Role
- Clarity, completeness, consistency and verifiability of functional requirements
- Accuracy, resolution and response time for all outputs
- Completeness of interface requirements
- Testability and self-supervision requirements
- Safety and security requirements
- Reliability and maintainability requirements
- Forward and backward Traceability with DBR

- ✓ Baselined Documents:
- System Requirements (SR)

System Architecture Review

✓ Documents submitted:

- System Design Guidelines (SDG)
- System Architecture Design (SAD)
- System Validation Procedure (SVP) (at Lab/Factory and at Site)
- System Integration and Test Procedure (SysITP)
- System Safety Analysis Report (SSAR)
- All Plans (PMP, SDP, CMP, HQAP, SQAP, HVVP and SVVP)

✓ Activity:

- All plans are reviewed for completeness and consistency.
- System Design Guidelines (SDG) are reviewed for applicability and consistency.
- Major traits reviewed for SAD:
  - Clarity, completeness and consistency of functional, performance, resource and interface (external and internal) requirements for each subsystem/package.
  - Cohesion and coupling
  - Conformance to SDG
  - Traceability to SR

System Architecture Review(Contd.)

- Major traits reviewed for System Integration and Test Procedure (SysITP):
  - Clarity, completeness and Traceability to SAD
- Major traits reviewed for System Validation Procedure (SVP):
  - Testability of all features/functions
  - Test setup requirements
  - Completeness, consistency and Traceability of test cases
- System Safety Analysis Report (SSAR) is reviewed for completeness and consistency.

✓ Baselined Documents:

- System Architecture Design (SAD)

Hardware/Software Specifications Review

- ✓ Documents submitted:
  - Hardware Requirements Specification (HRS)
  - Software Requirements Specification (SRS)
- ✓ Activity:

The major traits reviewed for HRS are:

- ➢ Clarity, completeness and testability of functional requirements
- ➢ Accuracy, response time and throughput
- ➢ Consistency with other hardware and software requirements
- ➢ Traceability with SAD

Hardware/Software Specs Review (Contd.)

The major traits reviewed for SRS are:

- ➢ Clarity, completeness.consistency, error handling / recovery and safe outputs
- ➢ Precision, accuracy and frequency of outputs
- ➢ Access control and data security
- ➢ Integrity checks
- ➢ Consistency with other hardware and software specifications
- ➢ Traceabilty to SAD

- ✓ Baselined Documents:
  - Hardware Requirements Specification (HRS)
  - Software Requirements Specification (SRS)

Hardware/Software Design Review

- ✓ Documents submitted:
- Hardware Design Description (HDD)
- Hardware Integration and Test Procedure (HITP)
- Hardware Reliability Analysis (HRA)
- Programming Guidelines (PG)
- Software Design Description (SDD)
- Software Integration and Test Procedure (SITP)

- ✓ Activity:

Hardware Design Review:

- HDD is examined for completeness, consistency and traceability with respect to HRS
- HITP should cover procedure for progressive integration and testing of various modules/subsystems and tests for all functional and performance specification given in HRS. It should also include the test setup
- HRA is reviewed for completeness and consistency.

Hardware/Software Design Review (Contd.)

Software Design Review:

- The Programming Guidelines (PG) are reviewed for their applicability and consistency
- The Software Design description (SDD) is reviewed for following traits:
  - ➢ Modularity
  - ➢ Cohesion and coupling
  - ➢ Nominal and maximal performance for each module
  - ➢ Error detection, containment and recovery
  - ➢ Traceability to SRS

- ✓ Baselined Documents:
- Hardware Design Description (HDD)
- Software Design Description (SDD)

Hardware/Software Implementation Review

- ✓ Documents submitted:
- Hardware Unit Test Report (HUTR)
- Hardware Integration and Test Report (HITR)
- Software Unit Test Report (SUTR)
- Software Implementation (Source and Object Code)
- Software Integration and Test Report (SITR)

- ✓ Activity:

Hardware Implementation Review:

- The HUTRs and HITR are reviewed for completeness and consistency

Hardware/Software Implementation Review (Contd)

Software Implementation Review:

- The SUTRs and SITR are reviewed for completeness and consistency
- The software source code is analyzed (through static analysis) to consider compliance to Programming Guidelines and complexity and other properties.
- Code walkthrough is carried out to confirm compliance to Programming Guidelines and correct implementation of the design as stated in SDD

- ✓ Baselined Documents:
- Software Code (SC)

System Integration Review

✓ Documents submitted:

- System Integration and Test Report (SysITR)
- System Build (SB)

✓ Activity:

- The SysITR and SB are reviewed for completeness and consistency

✓ Baselined Documents:

- System Build (SB)

System Validation

✓ Documents submitted:

- User Documentation (UD)

✓ Activity:

- UD is reviewed for completeness and consistency
- System is validated at Laboratory (using SVP) and IVVC issues System Validation report (SVR)
- System is validated at factory (using SVP for Factory and System Build) and IVVC issues System Validation report (SVR-F)
- System is validated at site (using SVP for Site and System Build) for correct assembly, connection to the plant and safe operation and IVVC issues System Validation Report (SVR-S)

✓ Baselined Documents:

- User Documentation (UD)

Summary

- Embedded systems need to be systematically engineered in accordance with established standards
- Software Quality Assurance is essential for ensuring dependability of embedded systems

THANK YOU