Verification and Validation for Advanced Train Control Systems

Gideon Ben-Yaacov

Verification and validation (V&V) techniques are used in military, space, nuclear power, and other industries to improve the quality of digital systems. V&V will ensure that quality advanced train control systems (ATCS) are implemented and that the ATCS will, indeed, provide the anticipated level of vitality. Railroads or system suppliers can use V&V programs when developing V&V procedures, plans, tasks, and activities for use during the implementation of ATCS.

Verification and validation (V&V) programs are vital for successful advanced train control systems (ATCS) design and performance. V&V processes can be applied to the overall ATCS, including the software, hardware, and user terminals.

The V&V program is defined in an implementation plan document that provides the recommended procedures and tasks to be followed when the V&V process is implemented. This document is also known as the system verification and validation plan document. The recommended V&V procedures apply to both vital and nonvital items of ATCS hardware and software. They are performed in parallel to ATCS development.

V&V should be performed by a group independent of the ATCS developer and supplier. The group should be designated at the beginning of the ATCS project and should be responsible for the following:

- Preparing a detailed V&V plan,
- Performing V&V activities as defined in the plan,
- Participating in development of a test plan, test procedures, and acceptance criteria,
- Witnessing system testings, and
- Evaluating test results.

If the ATCS are developed by outside suppliers and/or system integrators, the railroad companies should assign engineering staff as active participants on the V&V team.

The V&V activities can provide a comprehensive evaluation of each phase of the ATCS development project and help ensure the following:

- Deficiencies are detected and corrected as soon as possible in the ATCS life cycle.
- Probability of project risk, cost increase, and schedule delay is reduced or eliminated.
- ATCS quality and reliability are enhanced.
- Proper vitality features are provided with the ATCS.
- Management's knowledge of the ATCS developmental process is improved.
- Proposed changes/improvements and resulting consequences are assessed and monitored.

DEFINITIONS

The following are definitions of terms used in this paper.

- Required inputs—Items necessary to perform V&V tasks for each life-cycle phase of the system.
- Required outputs—Items resulting from performing V&V tasks for each life-cycle phase of the system.
- System integrated testing—Process of testing an integrated hardware and software system to verify that the system meets its specified requirements.
- Test plan—Documentation specifying the scope, approach, resources, and schedule of intended testing activities.
- Test procedures—Documentation detailing test procedures, inputs, predicted results, and execution conditions for each test item.
- Validation—Process of evaluating a system at the end of the development process to ensure compliance with functional and performance requirements. It is based on evaluating an integrated testing of hardware and software. The validation process provides assurance that the capabilities of the system, as described in the requirement specification document, are implemented in the hardware and software.
- Verification—Process of determining whether the product of a given phase of a system development cycle fulfills the requirements established for that phase. Verification is based on system development documentation. Verification ensures that an accurate translation of information from one phase of development to the next phase has been performed (for example, the review of design specifications ensures that the design meets functional requirements).

V&V IMPLEMENTATION PLAN

V&V tasks for a specific ATCS project are defined in an ATCS system verification and validation plan (SVVP). The tasks are intended to verify that the product of each ATCS development phase complies with the phase requirements for correctness, completeness, consistency, and accuracy and to validate that the completed ATCS complies with established requirements.

Automated Monitoring and Control International, Inc., 11819 Miami Street, Omaha, Nebr. 68164.

Figure 1 provides a summarized review of ATCS V&V activities as defined in a SVVP. The V&V input, tasks, and output for each ATCS life-cycle phase are identified. The ATCS life-cycle phases used in the SVVP are as follows:

- Concept,
- Requirement,
- Design,
- Implementation,
- Testing,
- Installation and checking, and
- Operation and maintenance.

Table 1 contains a description of the V&V tasks applicable to each project implementation phase as well as the inputs and outputs required to accomplish these tasks. The scope and contents of each section of the SVVP are described next.

1. *Purpose:* The purpose and scope of the proposed V&V plan and the project for which the plan is prepared are described.
2. *Reference documents:* Documents that support plan implementation are identified.
3. *Plan overview:* The organization, schedule, resources, responsibilities, and plan management methodologies necessary to perform ATCS V&V tasks are described.
4. *V&V tasks:* A detailed plan of V&V tasks throughout the ATCS life cycle is provided and includes the following:

(a) Specific V&V task(s) recommended for each phase,
(b) Methods and criteria used in performing each task,
(c) Inputs and outputs required for each task,
(d) Schedule for the tasks,
(e) Resources for performing the tasks,
(f) Roles and responsibilities of individuals responsible for performing the tasks, and
(g) Management of the tasks.

5. *V&V reporting:* The content and format of all V&V reports are described. The following types of reports are generated to support V&V activities:

(a) Deficiency reports are generated for each deficiency or abnormality detected by V&V. Each report contains a description of deficiency, the impact on ATCS operation and performance, the cause, the criticality, and recommendations.
(b) V&V phase summary reports contain summaries of the results of the specific V&V tasks performed for each life-cycle phase. Each report contains a description of the V&V task, a summary of task results, a summary of deficiencies and resolutions, an assessment of ATCS quality, and recommendations.
(c) V&V final report is issued at the end of the installation and checkout phase. It includes a summary of all V&V tasks, a summary of deficiencies and resolutions, an assessment of ATCS quality, and recommendations.

6. *V&V administrative procedures:* The following V&V administrative procedures are described: deficiency reporting and resolution, configuration management procedures, and standards, practices, and policies.

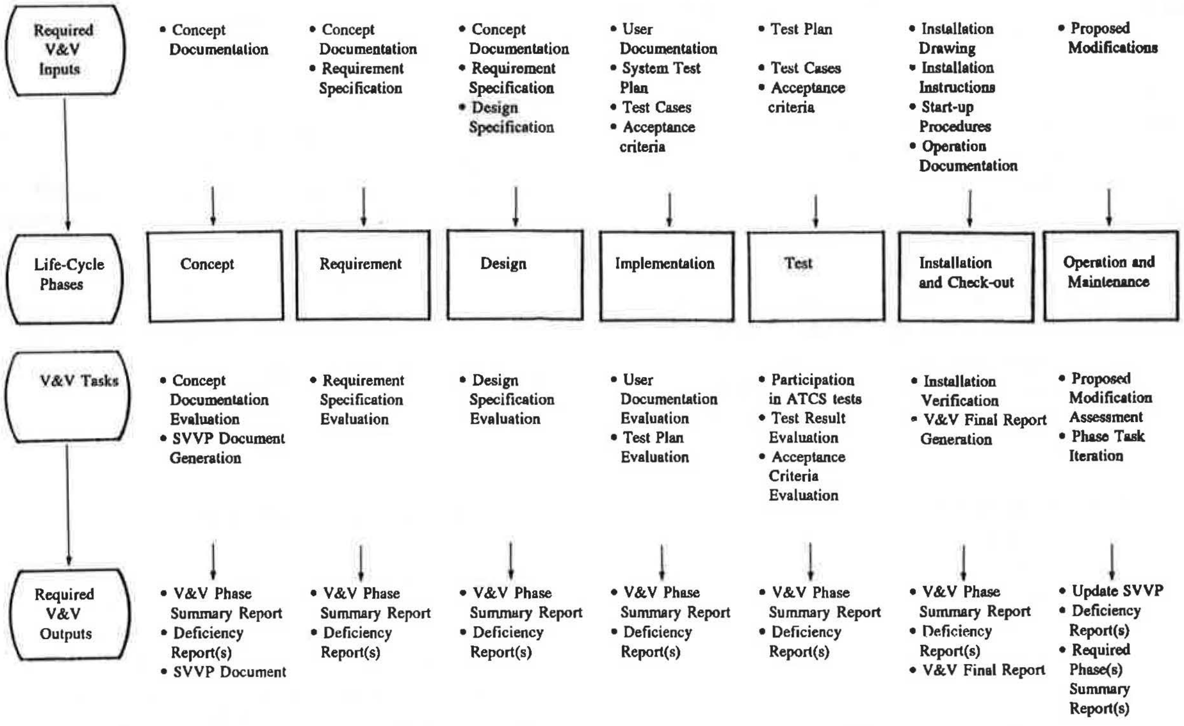
Required V&V Inputs
• Concept Documentation
• Concept Documentation
• Requirement Specification
• Concept Documentation
• Requirement Specification
• Design Specification
• User Documentation
• System Test Plan
• Test Cases
• Acceptance criteria
• Test Plan
• Test Cases
• Acceptance criteria
• Installation Drawing
• Installation Instructions
• Start-up Procedures
• Operation Documentation
• Proposed Modifications
Life-Cycle Phases
Concept
Requirement
Design
Implementation
Test
Installation and Check-out
Operation and Maintenance
V&V Tasks
• Concept Documentation Evaluation
• SVVP Document Generation
• Requirement Specification Evaluation
• Design Specification Evaluation
• User Documentation Evaluation
• Test Plan Evaluation
• Participation in ATCS tests
• Test Result Evaluation
• Acceptance Criteria Evaluation
• Installation Verification
• V&V Final Report Generation
• Proposed Modification Assessment
• Phase Task Iteration
Required V&V Outputs
• V&V Phase Summary Report
• Deficiency Report(s)
• SVVP Document
• V&V Phase Summary Report
• Deficiency Report(s)
• V&V Phase Summary Report
• Deficiency Report(s)
• V&V Phase Summary Report
• Deficiency Report(s)
• V&V Phase Summary Report
• Deficiency Report(s)
• V&V Phase Summary Report
• Deficiency Report(s)
• V&V Final Report
• Update SVVP
• Deficiency Report(s)
• Required Phase(s) Summary Report(s)

FIGURE 1 V&V plan overview.

TABLE 1 V&V TASKS, INPUTS, AND OUTPUTS FOR ATCS LIFE-CYCLE PHASES

V&V TASKS	REQUIRED INPUTS	REQUIRED OUTPUTS
V&V PLAN		
ATCS Verification and Validation Plan (SVVP) Generation During Concept Phase, the SVVP is generated for all ATCS' life-cycle phases. The SVVP should be considered to be a "Living" document, and changes are made as needed.	● Project implementation Schedule ● Concept documentation	● SVVP Document
Concept Documentation Evaluation Concept documentation is evaluated to determine if proposed concepts satisfy user needs and project objectives. Major constraints of interfacing subsystems and limitation of proposed approach are identified.	● Concept documentation (for example, Statement of Need, Advance Planning Report, Project Initiation Memo, Feasibility Study, ATCS Definition Document)	● Deficiency report(s) ● V&V Phase Summary Report
REQUIREMENT PHASE V&V		
Requirement Evaluation ATCS functional requirement specification is evaluated for correctness consistency, completeness, accuracy, readability, and testability. The ATCS requirement specification is to be assessed as to how well it satisfies railroad's objectives and user needs as defined in the Concept documentation.	● Concept Documentation ● ATCS functional requirement documentation (for example, ATCS requirement specification, request for proposals, proposals, contract documentation, etc.)	● Deficiency report(s) ● V&V Phase Summary Report
DESIGN PHASE V&V		
Design Evaluation ATCS design specifications are evaluated for correctness, consistency, completeness, accuracy, and testability. The ATCS design specifications are assessed as to how well they satisfy ATCS objectives as outlined in the ATCS requirement specification.	● ATCS Requirement Specification document ● ATCS Design Specification document	● Deficiency report(s) ● V&V Phase Summary Report
IMPLEMENTATION PHASE V&V		
ATCS Test Plan Evaluation ATCS test plan is evaluated to determine whether it provides a suitable plan for ATCS testings.	• ATCS Test Plan Document	• Deficiency report(s)
ATCS Test Procedure Evaluation ATCS test procedures are evaluated to determine whether the procedures are adequate for subassembly testing, integration testing, and acceptance testing.	• ATCS Test Plan Document • ATCS Test Procedure Documents	• Deficiency report(s) • V&V Phase Summary Report
TEST PHASE V&V		
Testing ATCS testing is witnessed by a member(s) of the V&V team who would assist in recording all testing results as required by the Test Plan.	• Test Plan Document • Test Procedure Document	• Deficiency report(s)
Test Analysis ATCS test results are analyzed to determine whether the ATCS satisfies acceptance criteria.	• Test Plan Document • Test Procedure Document • Test Results	• Deficiency report(s) • V&V Phase Summary Report
INSTALLATION AND CHECKOUT PHASE V&V		
Installation Audit ATCS Installation is audited to determine that all equipment, software, and cables are correctly installed and operational. instructions.	• Installation documentation (for example, installation drawings, installation procedures, installation tests, diagnostics, start-up procedures, operational procedures)	• Deficiency report(s) • V&V Phase Summary Report
V&V Final Report Generation All V&V activities and results are summarized in this report.	• All V&V Phase Summary Reports	• V&V Final Report
OPERATION AND MAINTENANCE PHASE V&V		
V&V Plan Revision The ATCS SVVP document will be revised, as necessary, to be	• SVVP document	• Updated SVVP
Proposed Modification Assessment All approved modifications, enhancements, or additions will be assessed to determine the effect each modification would have on V&V tasks. The extent to which V&V tasks would be iterated will be determined. These V&V tasks are aimed to insure that each planned modification is implemented correctly.	• Approved modification(s)	• Scope of V&V tasks required to support the modification(s)
Phase Task Iteration For each approved modification, the specific V&V tasks required to support the modification will be performed.	• Approved modification(s)	• Deficiency report(s) • Required phased outputs of iterated tasks

V&V MANDATORY ACTIVITIES

V&V activities are an integral part of the quality assurance process used to finalize the functional specification requirements, design, building, testing, installation, and acceptance of the ATCS. V&V activities are, therefore, integrated into the ATCS project activities.

Some of the V&V activities are extremely beneficial and, therefore, are considered mandatory, whereas others are viewed as desirable and, therefore, considered optional. Mandatory tasks are performed during the requirement (verification of ATCS requirements), design (verification of ATCS design), testing (ATCS validation), installation and checkout (verification of ATCS installation), and operation and maintenance (V&V of ATCS modifications and upgrades) phases.

These mandatory activities are as follows:

1. *Verification of the ATCS requirement:* During this verification process the ATCS requirement specification document is reviewed. The main objective is to determine whether the ATCS requirements are complete, understandable, consistent, feasible, and testable. This review should be performed before the detailed design and development of hardware and software.
2. *Verification of the ATCS design:* This verification process consists of a review of the ATCS design specification document. The review of the hardware and software designs focuses on determining whether the designs are a correct implementation of ATCS requirements.
3. *ATCS validation:* The ATCS validation consists of testing to validate that the complete ATCS is a correct implementation of the ATCS requirement specification.
4. *Field verification:* The field verification consists of testing field installations to ensure that the ATCS has been properly installed.
5. *Operation and maintenance V&V:* This activity supports all future upgrading and modifications of the ATCS.

These five mandatory V&V activities for an ATCS development project are further described in the following paragraphs.

Verification of ATCS Requirements

The system requirements are the foundation on which the ATCS is designed, built, and accepted. System requirements are verified through a review of the ATCS requirement specification document for correctness, completeness, consistency, understandability, feasibility, testability, and traceability. The verification of the ATCS requirement specification is perhaps the most important V&V activity. Its principal goal is to determine independently that the ATCS requirements result in a practical solution to the railroad's objectives. The ATCS requirement verification addresses the following:

- Completeness and correctness in specifying the functional capability and performance requirements of the ATCS;
- Completeness and correctness in specifying the internal interfaces within the ATCS and the external interfaces to the railroad's corporate computers;
- Unambiguous, correct, and consistent description of the functional characteristics and performance for each major subsystem and/or software package;
- Reasonable, achievable, and suitable ATCS test requirements;
- Definitions of subsystems' physical characteristics, reliability and maintainability objectives, operating environments, and design and development standards;
- User interface requirements; and
- Definition of installation, operation, training, documentation, and maintenance requirements.

The results of the ATCS requirement specification document review are recorded in a V&V report. Typical contents of this requirement verification report are as follows:

- Background:
  - –Identification of the ATCS requirement specification document,
  - –Identification of other referenced documents, and
  - –Review participants;
- Results of review:
  - –Functional requirements,
  - –Definition and interfaces,
  - –Design requirements,
  - –Operational environments,
  - –Test requirements and acceptance criteria,
  - –Supporting services requirements (i.e., training, documentation, etc.),
  - –Performance requirements,
  - –Installation requirements,
  - –Operational capabilities,
  - –Maintenance, and
  - –Other requirements;
- Attributes:
  - –Correctness,
  - –Completeness,
  - –Consistence,
  - –Understandability,
  - –Feasibility,
  - –Testability, and
  - –Traceability; and
- Summary of deficiencies to be resolved.

Verification of ATCS Design

Verification of ATCS design is performed through the review of the ATCS design specification. The ATCS design specifications are reviewed to ensure that the ATCS functional requirements, implemented by the hardware and software designs, are complied with and that there are no ambiguities or deficiencies. The design review examines the design of the hardware and software in terms of their ability to satisfy performance and functional requirements:

- Architecture (both hardware and software);
- Major equipment interfaces;
- Operating procedures (initialization, start-up, error detection, restart, etc.);
- Testability (use of test equipment such as simulations);
- Timing analysis (display response time, communication response time, etc.);

- Availability (reliability prediction report indicators);
- Information flow (data communication between major hardware components); and
- Human factors (analysis performed to evaluate layout and contents of user's interfaces).

The ATCS design specification documents are usually more detailed than the system requirement specification document. They detail how the requirements are met. One of the key objectives of design verification is to ensure that the ATCS design is consistent with the ATCS requirements. The design review, therefore, will provide an independent assessment of the ability of the design to meet functional and performance requirements. Such capabilities as response time, availability, man-machine interface, data quality, operating environments, and testability must be analyzed as part of the design evaluation. The V&V team will review the information contained in the design specification documentation for correctness, feasibility, and consistency. Some of the performance requirements may be difficult to ascertain, but it is more efficient to identify these issues during the design phase than later during the validation testing.

Another result of the design review is the evaluation of test requirements and criteria. This information is useful for the evaluation of the ATCS test procedures aimed at validating ATCS performance and capabilities. Furthermore, the evaluation of test requirements and criteria ensures that the ATCS is designed to be testable and that a test plan can be efficiently developed.

The results of the design verification activity are documented. Any deficiencies are identified. Information provided in the design verification report is as follows:

- Background:
  - –Identification of the ATCS design specification documents,
  - –Identification of other referenced documentation, and
  - –Review participants;
- Results of review:
  - –ATCS hardware and software architecture,
  - –Hardware subsystem interfaces (including isolation, signal type and rates, protocols, etc.),
  - –Hardware subsystem design,
  - –Software subsystem design (including operating systems, applications, utility programs, priorities, error control/recoveries, algorithms, etc.),
  - –ATCS hardware and software integrated testing, and
  - –Human factor engineering;
- Attributes:
  - –Design completeness,
  - –Design consistence,
  - –Hardware/software testability,
  - –Design traceability, and
  - –User acceptability; and
- Summary of deficiencies to be resolved.

ATCS Validation

ATCS validation is accomplished through extensive ATCS testing. This testing demonstrates that the integrated ATCS meets the functional and performance requirements described in the ATCS functional specification document. Four activities are associated with ATCS validation testing: (a) Test plan review, (b) ATCS test procedures review, (c) participation in ATCS test execution, and (d) analysis of test results. The test results, analysis, and nonconformances to acceptability criteria are documented in a validation test report. Typical contents of such a report are as follows:

- Background:
  - –Purpose of tests,
  - –Summary of test plan, and
  - –Reference documents;
- Analysis of test results:
  - –Test environment and configuration,
  - –Test results collected,
  - –Acceptance criteria,
  - –Test results analysis,
  - –Actions to be taken, and
  - –Conclusions;
- Summary:
  - –Capabilities demonstrated and
  - –ATCS deficiencies; and
- Recommendations:
  - –ATCS refinements and
  - –Further testing.

Field Verification

Field verification ensures that the ATCS has been properly installed. The installation procedures, drawings, and start-up procedures are reviewed by the V&V team. Field verification entails stationary tests of all system cables, mechanical constructions, and software installations to ensure that all ATCS components are properly installed.

Field verification activities are defined in a field verification plan, which is included in the SVVP. The plan identifies the methods used to verify proper installation and the environments of the various subsystems. Analysis of field verification results is documented in the field verification analysis report. Typical contents of such a report are as follows:

- Background:
  - –Purpose of field verification,
  - –Summary of field verification activities, and
  - –Reference documents;
- Analysis of results:
  - –Completeness of installation drawings and start-up procedures,
  - –Verification of proper installation of system cables,
  - –Verification of proper installation of hardware devices,
  - –Verification of proper mechanical construction, and
  - –Verification of proper installation of system software (including utilities, diagnostics, operating systems, firmware, etc.);
- Summary:
  - –Installation deficiencies and
  - –Actions to be taken; and
- Recommendations:
  - –Correction of deficiencies and
  - –Further verification of installation work that will be redone.

Operation and Maintenance Phase V&V

As experience is gained in the operation and maintenance of the ATCS, improvements and modifications will be made. Such modifications may entail a new requirement or capability, or a design modification that improves performance, usability, or reliability. Once the scope of a modification is defined and approved, the V&V implementation phases for the modification are similar to those used during ATCS development.

The V&V for ATCS modifications will depend on the type and extent of each modification. For example, for minor modifications such as a format change on the on-board display, it may consist merely of noting the result of the change. Modifications that significantly affect the performance or the functional capability of the ATCS will require more detailed V&V.

CONCLUSION

Providing state-of-the-art technology for train control and monitoring involves greater risk than using the traditional field-proven signaling system. A major reason for this is that ATCS subsystems are based on newly developed products and software and are built according to an individual railroad's specific requirements, vendors' specific design specifications, and the North American railroads' generic ATCS specifications. The V&V process described in this paper reduces the risk associated with newly developed ATCS.

V&V is a process of review, analysis, and testing employed throughout the ATCS development life cycle. It provides a way to ensure successful ATCS implementation, thereby providing an increased level of confidence in ATCS design, development, and implementation. Through a series of checkpoints and reviews, V&V, as a methodology, helps ensure that quality ATCS systems are implemented.

Verification, through documentation review, is performed at each phase of the ATCS development life cycle. It determines that each phase product is correct, complete, and consistent with itself and with predecessor products. Validation, through testing and analysis, determines the correctness of the end product (i.e., the entire ATCS) with respect to ATCS requirement and design specification.

The recommended V&V activities provide a comprehensive set of tasks aimed at enhancing the quality of the entire range of ATCS development phases. Proper implementation of the recommended V&V process will result in the following:

- Safe train operation under ATCS,
- Accurate cost estimating and schedule planning,
- Understanding of the ATCS requirements,
- Adequate testing of the ATCS,
- Proper documentation of the ATCS,
- Satisfactory ATCS performance,
- Use of sound human factors engineering practices,
- User participation in ATCS development,
- Management control during ATCS development, and
- Achievement of anticipated benefits.

The level of V&V effort appropriate for an ATCS implementation project described in this paper is considered adequate to provide confidence that the ATCS can perform its functions in a satisfactory manner. However, the effort level is not extensive as to create unnecessary delays in the development and implementation of the ATCS. The main goal of the recommended level of V&V is to provide results in areas where most benefits can be obtained. It is believed that the recommended level of effort is sufficient to meet the intent of the recommended V&V process stated in ANSI/IEEE Standard 1012 for developing V&V plans for both critical and noncritical software.