Challenges Of Vital Overlay System Acquisition

Linda Martinez, CSEP
SYSTRA Engineering, Inc.
New York, NY

ABSTRACT

Safety is a top priority of federal agencies, rail transit agencies, railroads, and the public. Acquisition of a new safety-critical or vital rail system requires a thorough specification of functional, operational, maintenance, performance, and program requirements. A comprehensive System Safety Program is required to be implemented and safety quantified for the entire system. Once an acceptable level of system safety has been achieved it must be maintained for the life of that system.

What must be considered in the specification for a safety-critical or vital system to be implemented to operate as an overlay to an existing safety-critical or vital system? This paper will look the challenges of specifying the requirements for implementing and verifying system safety of the new vital functions while maintaining the safety of the underlying system.

INTRODUCTION

Railroads around the world have come a long way from wooden tracks and steam engine locomotives to the advanced infrastructures and systems that make up today's railroad operations. Over the last century the safety of train operation has been continuously improving, introducing electronic systems that provide warning to the crew or initiate controls to intervene in unsafe situations. Today's railroad systems include microprocessor based interlockings, cab signal systems, automatic train control, automatic train stop systems and others. However these advancements didn't progress in the US without the heeding from regulatory bodies and after deadly accidents were attributed to human error.

Following one such accident, the collision between a Boston and Maine Corporation commuter train and a Consolidated Rail Incorporated (CONRAIL) freight train in May 1987, the National Transportation Safety Board (NTSB) drafted the initial "Most Wanted List of Transportation Safety Improvements" in 1990. Among the improvements recommended by the NTSB to the Federal Railroad Administration (FRA) was the installation and operation of a new train control system that would ensure positive train separation.

Recognizing the need for improved safety systems for our railroads however is not enough to push forward to realization. There are several factors that must be considered and aligned in order to result in change including availability of technology, viability of rule changes, financial resources, and of course federal regulations. Maintaining and repairing our railroad infrastructure demanded most of the capital resources, until the 1980's microprocessor based systems hadn't matured, and the regulations were in their infancy. Most unsafe conditions were attempted to be mitigated through operation changes; with the root of most accidents as human error the opportunity for safety improvement without technology improvements however eventually hit a wall.

Through the late 20th and early 21st century railroads, suppliers, and the FRA worked together to develop and implement railroad improvements, unfortunately collisions, derailments, and work zone incursions continued. Two accidents in particular resulted in Congress mandating the implementation of what is now referred to as Positive Train Control or PTC Systems. The first accident was the January 6, 2005 collision of two freight trains in Graniteville, South Carolina resulting in 9 deaths and hazardous material contamination within a mile of the crash site and the second occurred on September 12, 2008 in Chatsworth, California where a freight train collided head-on with a commuter train resulting in 25 deaths. It became clear to the FRA that federal regulations were necessary to implement collision avoidance systems to overcome errors in operation and Congress passed the Rail Safety Improvement Act of 2008 (RSIA08) into law on October 16, 2008 amending several parts of title 49, Code of Federal Regulations (CFR) most notably Part 236 with the addition of Subpart I, Positive Train Control Systems (49CFR236I).

With the passing of RSIA08, a very aggressive schedule for the planning, implementation, and approval of PTC by each railroad subject to FRA regulations was established. 49CFR236I mandated that a PTC system be FRA approved and installed by December 31, 2015[1]. The schedule included delivery of a PTC Implementation Plan (PTCIP) by each railroad defining for FRA approval how the railroad planned to implement PTC systems including what technology would be used and any territory exclusions. Following the approval of the PTCIP by the FRA, railroads would further define the plan for how PTC would be developed as part of a PTC Development Plan (PTCDP). Finally, because ultimately the RSIA08 was instituted to make our railroad operation safer, an FRA approved PTC Safety Plan (PTCSP) providing evidence that the PTC is safe (or at least as safe as the current operation) was required to be approved by the railroad before the Dec. 2015 date. Railroads found that they had little time to investigate and analyze new implementation concepts, had to consider interoperability between adjacent railroads, maintain capacity and safety, and burden already strained capital programs with the high cost of PTC.

VITAL PTC OVERLAY

With little time for developing new or modified systems that would replace current train control to include PTC, railroads had to look at what was already available. The purpose of this paper is not to look at the evolution of PTC systems or to describe in detail PTC functionality. Instead this paper looks at applying Systems Engineering to specifying a specific type of PTC implementation, as an overlay to an existing railroad. One critical component of any overlay system, that is one that 'sits atop' of another system, is that the underlying system must be preserved without compromise. Where that underlying system is a vital system, one that is not only safety critical but which under all states must never fail in an unsafe or unknown state, introducing any new interfacing or operating system in the same environment presents opportunity for degrading safety.

There were several existing PTC systems available at the time of RSIA08, however this paper utilizes the Advanced Civil Speed Enforcement System II (ACSES II) developed and implemented by AMTRAK as the example. The ACSES II PTC was Type Approved by the FRA on May 27, 2010[2] which made it a viable option for meeting PTC regulations for other railroads.

Considering a railroad that operates with existing onboard Automatic Train Control (ATC) and microprocessor-based signal system, PTC is designed to prevent train-to-train collisions, overspeed derailments, incursions into established work zone limits, and movement of a train through a switch left in the wrong position. The application of ACSES II does not involve modification to the existing ATC or re-signaling, but the challenges of application are equally demanding. The resulting signal system operating with the PTC overlay must maintain existing safety integrity, service capacity while not introducing train delay, and during implementation limit impacts to operation. Additionally within a railroad system, PTC must be interoperable with all equipped trains that run on the system and with adjacent systems that the railroad's trains traverse.

Implementation Challenges

Implementing a vital (or safety-critical) system is challenging, but that challenge is increased when the new vital system is overlaid on another operating vital system. The underlying signal system is independent of the PTC but the PTC is reliant on the underlying signal system. Additionally although the existing systems are independent of PTC, the overall operation is integrated. Engineering the overlay system therefore must maintain a whole system focus as well as a 'PTC-only' focus to define the performance goals, functional requirements, operational scenarios, implementation strategy, verification and validation, and demonstration of safe operation necessary to ensure vitality and in the case of PTC meet FRA regulations. Selecting to implement ACSES II does provide a basis of safety from the AMTRAK Type Approval. However as all railroads operate differently, have different infrastructures and systems, and have different needs modifications to the already FRA approved ACSES PTC system becomes inevitable. With change comes the need for certification and FRA approval of safe operation.

PTC is made up of several systems and subsystems working together to provide the required functions. Figure 1 depicts a configuration of ACSES II equipment performing specific functions of the PTC. Existing equipment and interfaces are shown (highlighted)

[1] FRA has recommended to Congress extending the PTC implementation deadline

[2] Federal Railroad Administration Type Approval #FRA-TA-2010-001

including ATC and wayside signals, switches, and track circuits. The PTC subsystems are defined as follows:

- Back Office: Vital management of Temporary Speed Restrictions (TSR) and dispatcher TSR entry
- Towers: remote TSR entry
- Onboard vehicles: Vital ACSES Onboard Computer (OBC) that processes data obtained from transponders and via a mobile data radio (MCP) to enforce permanent and temporary speed restrictions and positive stops short of targets.
- Interlockings: Vital Wayside Interface Units (WIU) providing interface to the existing vital signaling system; Base Communication Packages (BCP) providing data radio transmission between the wayside and trains and communication between the wayside and office via the a Backbone Communications Network
- In-Track: Passive Transponders that cause the OBC to request WIU data and TSR data.

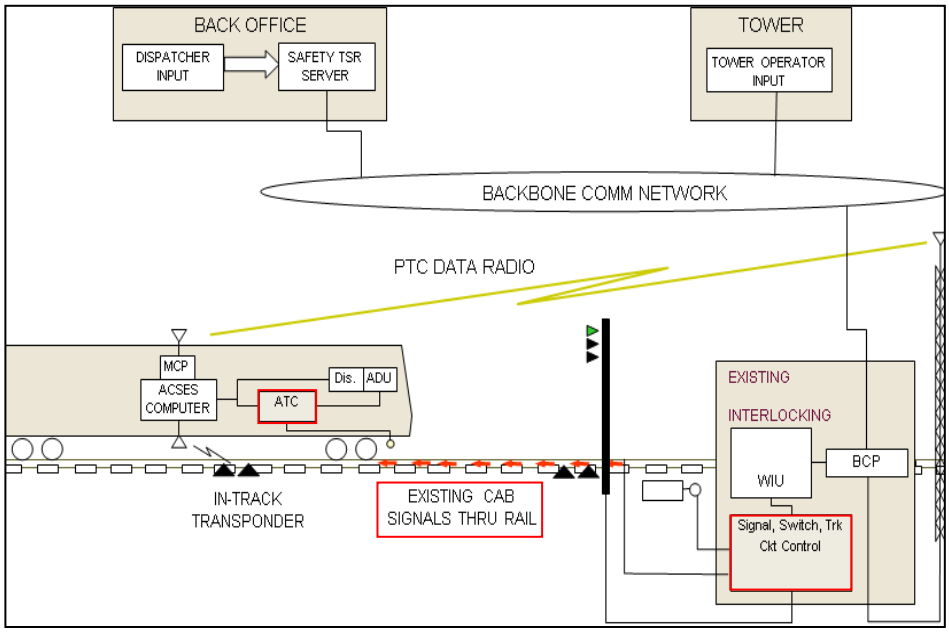

Figure 1: PTC System Configuration

Implementing PTC on an operating passenger railroad is akin to modifying the signal system in that the configuration of PTC encompasses locations throughout the entire system to support continuous train movement. Additionally all vehicles must be equipped to communicate with the wayside. The implementation challenge is the same, how to install and test PTC while continuing to provide uninterrupted, safe service for all trains including tenants (railroad operating in another railroad territory). Taking lessons learned from re-signaling, implementation must be done on a segmented basis (or line basis) allowing both PTC equipped and unequipped trains to operate on implemented PTC segments as they become available. Existing operation must be maintained throughout the entire system however as PTC operation becomes available in the implemented segments for equipped trains. As more vehicles become PTC equipped and additional segments are implemented, PTC operation is extended until complete.

Passenger railroads typically operate multiple vehicle types and are made up of multiple track configurations, grade crossings, stations, and other topographical features. A single solution design therefore is necessary to support the entire railroad, configurable for each specific implementation location. This raises the issue of a complete design and verification prior to full implementation to avoid re-design and re-testing if problems are uncovered in later segments. Design must be highly configurable to accommodate the different topology (i.e., braking distances, distance to next signal). Verification must be done as part of the earliest segments or separate 'pilot' segment(s) that include all vehicle types (i.e., interface with various existing onboard systems) and track configurations. The PTC solution must be tested and verified as a complete design, as part of the pilot segment(s).

The final challenge to implementing PTC is interoperability with tenant railroads. For ACSES II PTC on a commuter railroad, the ability to interoperate with adjacent railroads that share track for operation is mandated by 49CFR236I. That means that the implementation of PTC for a host railroad must provide for the sharing of TSR data with adjacent railroads to support seamless transition of trains across railroad boundaries. A means of communicating TSRs from one railroad PTC system to another PTC system becomes a challenging

function that extends the set of stakeholders for any given railroad PTC project to include those tenant railroads.

SYSTEMS ENGINEERING THE SOLUTION

The underlying signal system exists, onboard ATC exists, ACSES II design and products exist, and the railroad operating rules exist. Together they all form pieces of a puzzle that must be carefully put together to form the complete PTC picture for the railroad. Fitting the pieces requires careful alignment of the edges or 'interfaces' where the pieces meet to be sure that the final picture is complete and seamless. Starting with a whole picture of the final signal system + PTC is necessary to select the right pieces initially so they can be align properly from the start. Systems Engineering provides the practice and processes to define that final picture at the start and deliver the implemented solution at the finish to the satisfaction of all stakeholders, including the FRA.

advancing the state of the art and practice of Systems Engineering has done significant work in defining a quality, comprehensive guide for Systems Engineering. The most recent version of the guide, "INCOSE Systems Engineering Handbook", Version 3.2.2 (SEgbk) was published in Dec. 2011[3]. SEgbk is consistent with ISO/IEC 15288:2008 – *Systems and Software Engineering – System Life Cycle Processes* for application and usefulness across multiple domains. The development life-cycle and the processes defined through SEgbk and ISO/IEC 15288 are applicable across all industries, worldwide and includes a large basis of experience for all types of systems, including safety-critical systems.

Using the INCOSE model (Vee model) as the basis for understanding the activities and phases that are needed to specify the PTC system is the approach described in this paper. The groundwork for the PTC functionality and criteria for measuring success of the project are defined

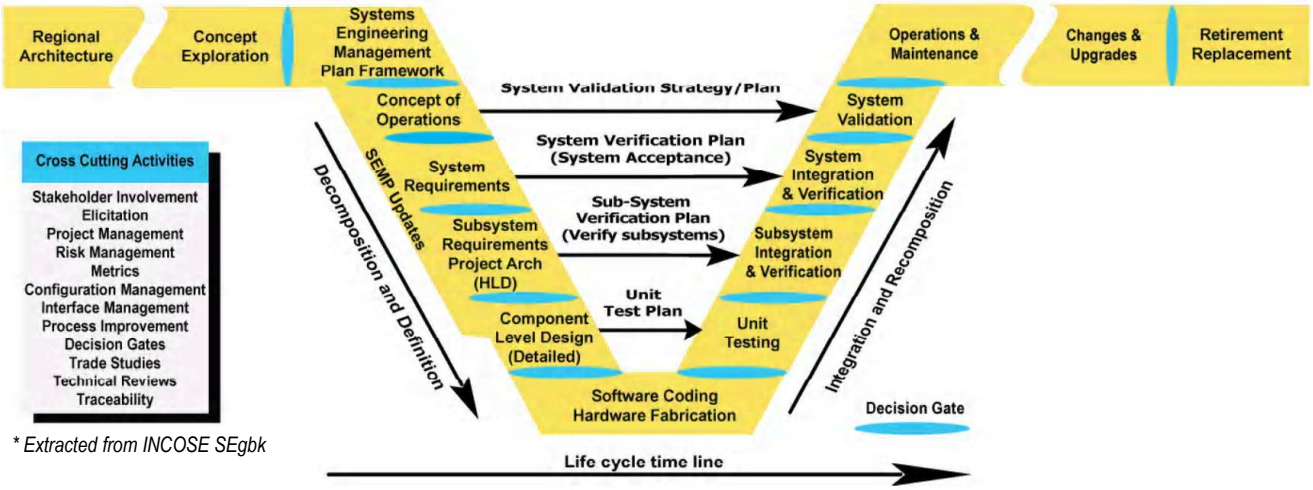

Figure 2: INCOSE Systems Engineering Vee Model

Systems Engineering integrates all disciplines and specialty groups together into a project following a structured process from concept to system acceptance with the goal of meeting all user needs and PTC requirements. Synthesizing transit knowledge domains that understand signaling, operations, communications, reliability, and system safety (among others) with the Systems Engineering (SE) domain that understands the process necessary to achieve the goals is the best solution to meeting the challenges inherent in acquisition of complex systems.

The International Council on Systems Engineering (INCOSE), a non-profit organization dedicated to

by the FRA 49CFR236I regulations and through the cited standards within those regulations. Assuring the safety of the PTC System is directed 49CFR236I through all phases of the project life-cycle; system safety assurance is integrated with the SE processes.

Because safety is not a 'one time' demonstration or measure, it is a crucial characteristic of a product that must be maintained and assessed well beyond the initial satisfaction of the FRA. By integrating safety into the SE

[3] Available through www.incose.org

life-cycle processes, it is not an "add on" to the system acquisition process; it becomes a fundamental component. Investing in safety early in the project life-cycle ensures production of systems that are inherently safe with minimal operational safety requirements or restrictions.

Systems Engineering Model

For an acquisition project such as PTC, where an owner defines a specification to hire a team to develop and implement the system through acceptance, the basic SE processes and relevant activities can be defined into four stages: concept (specification development), implementation (contracted team development and production), utilization (operation of system), and maintenance (which includes support and retirement), as shown in Figure 3. The Vee model is read from the top left down, then up the right side through retirement of the system at the top right.

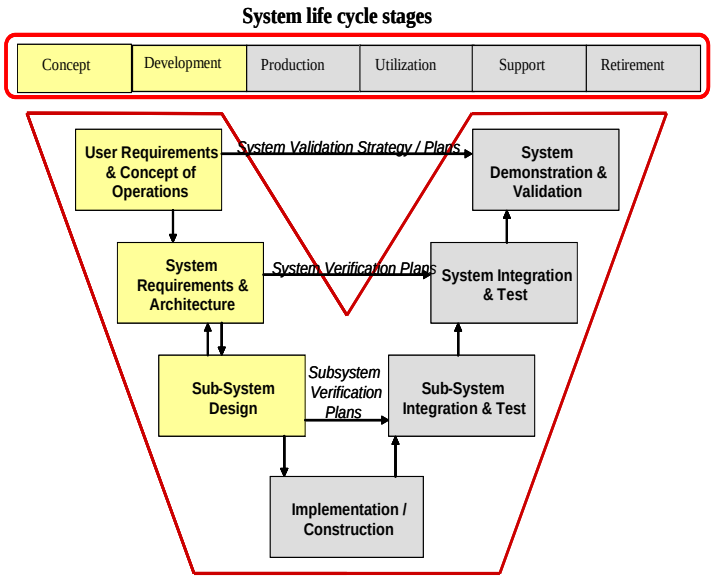

Figure 3: Simplified Vee Model and Life-Cycle

SE envisions the final system as a whole which goes beyond just the hardware and software that make up the PTC solution. It also includes all aspects of managing the project during implementation, delivering the evidence necessary for FRA approvals, tools necessary for the railroad to maintain the system through retirement, and the training program for all operation and maintenance staff through the life of the system. This whole system thinking is performed during the concept stage with a multi-disciplined team to ensure all elements of the system and project are clearly defined. It's not accidental that the Vee forms a flat edge at the beginning and the end (refer to Figure 2), as this whole system defined during the conceptual stages (upper left) are realized by the delivered system operated and maintained through retirement (upper right).

Systems Engineers meet with stakeholders to elicit the system and project needs, including the railroad, FRA, and tenant railroads. The needs are translated into a set of functional and project requirements that make up the specification for the system. The necessary activities for the implementation of the system to meet the functional and project needs are defined relative to the remaining life-cycle activities, development through retirement. Once the specification for the PTC System has been completed, the railroad can select a development team that will design the final PTC solution starting with the architecture and decomposing it down through multiple levels of design until the lowest component level is defined. These system analysis/design activities are represented by the left side of the Vee model, the bottom of the Vee represents the system implementation and construction.

The activities on the right side of the Vee represent the construction, test, and acceptance of the final product before moving to operation and maintenance. The right side of the Vee includes verification and validation (V&V) activities (i.e., tests and inspections) that proceed from the smallest units (at implementation) and build successively through the integration of subsystems (sub-system design) and systems (architecture design) as a systematic process, until the entire system is validated against the needs, requirements, and success criteria established at the start of the project (during Concept). For PTC, design and implementation activities (left side of Vee) are executed once for the full solution, the construction and V&V (right side of Vee) is performed for each segment until all segments are complete.

VITAL PTC SPECIFICATION

Once 49CFR236I was issued, the 'Concept' phase of PTC development began with the railroads. In order to successfully implement the vital PTC system it became necessary to understand not only the functions that PTC must provide but also the criteria by which to measure the success of the project. In the case of PTC, success is measured not only at completion but at checkpoints defined by the FRA. The specification for the PTC System must define these functional and project execution requirements to ensure each of the project criteria are met.

For the PTC the following key success criteria were defined:

- FRA approval of this PTC Implementation Plan (PTCIP) without required modification or re-submission.
- Implementation of design, procurement, and construction program elements according to the schedule.
- Reliable assertion of all PTC functions.
- Reliable Host/Tenant integration of PTC.
- Achieve FRA system safety certification upon initial FRA review.
- Successful commissioning of PTC on segments at the earliest possible dates consistent with meeting safety goals and minimal adverse impacts to operations.
- Completion of PTC implementation prior to December 31, 2015 deadline as currently mandated by §236.1011(a)(7).
- Completion of all employee operational and maintenance training in a timeframe consistent with the commissioning program.
- Accurate documentation and system configurations associated with the PTC system.

Decisions were made after considering alternatives to meet each item and the specification is developed to include the necessary requirements to ensure each criterion would be met. What follows is a summarization of the system thinking for each item, activities to be performed and responsible parties, phases of the system life-cycle affected, and finally means to measure success of the criteria.

Success Criteria: FRA Approval of PTCIP

The plan to implement PTC, as new development or implementation of an existing solution, was required to be submitted and approved by the FRA before starting any development activities. All viable solutions were investigated and in the case of this example an existing overlay of ACSES II was selected. Success is measured by submission to and approval by the FRA by the mandated date.

- What technology will be used?
- Single contract or multiple contracts?
- Who will act as the systems integrator for multiple contracts?
- How will FRA compliance be met?
- How will interoperability be provided between the host railroad and tenant railroad?
- Deployment sequence and schedule
- Justification for excluding any railroad mainline track from PTC?

Success Criteria: Complete To Schedule

In order to ensure that PTC implementation will successfully complete by the mandated FRA timeframes three major activities must be undertaken: FRA approval of the PTCDP, specification of the functionality and all project elements, and management of the implementation according to the specification. The activities and processes necessary to complete implementation by the mandated schedule apply to all life-cycle stages including procurement, design, and construction. Success is measured by the approval of the PTCDP and successful completion of all segments to the approved schedule.

- PTCDP: The plan to develop and implement the approved solution by Dec. 2015 is submitted and approved by the FRA before starting any development.
  - Conceptual configuration of PTC for the entire railroad territory
  - Safety goals and assumptions, including safety of the existing system
    - Must be at least as safe as the existing system
    - PTC Preliminary Hazard Analysis
    - FRA Type Approved ACSES II Safety Case
  - Reliability and availability goals and assumptions
    - PTC Reliability Analysis
    - Operational Performance Analysis
    - Reliability of FRA Type Approved ACSES II
  - Operating and maintenance scenarios
- Project and Implementation Elements: In order to achieve implementation a schedule must be defined and activities required that will allow for the monitoring and assurance against measurable milestones. Decisions must be made based on review of submitted documentation specific to the phase at milestone points (or decision points)

during the implementation to ensure agreement across the project before moving to the next phase.

- Design criteria, including hardware, software, and user interface standards
- Project Management Plan and Contracting Team Personnel
- Project Schedule including Phases and Milestone Reviews
- Deliverables
- Quality Management System including Failure Review, Change Control, and Safety Certification
- Managing Tools
  - Requirements Management
  - Configuration and Change Management
  - Failures Reporting and Corrective Action System (FRACAS)
  - Diagnostics and Test

Success Criteria: Reliable PTC Functionality

For PTC, the minimum functionality is defined by 49CFR236I and by the functionality provided by a selected existing solution (in this case ACSES II). However, in order to meet the specific needs of the railroad the Systems Engineer defines the additional railroad needs into the final set of PTC functionality. Integration of PTC into the railroad operation to ensure continued, safe operation is a major consideration. Success is measured through demonstration of all functionality under all operating and maintenance scenarios, safety certification by FRA, and demonstrating reliability and availability goals are met or exceeded for each subsystem and the system as a whole through operation.

- Gap analysis between ACSES II and railroad specific needs, ex. Vital scheduling of TSRs, Front of Train Determination
- Operational Availability Analysis: performance based analysis of current operation (i.e. train delays) using failure probabilities of ACSES II subsystems to determine impact (and mitigation) to train delay
- Preliminary Hazard Analysis including Mitigations
- Pilot Phase: define initial segments as track that includes all configuration types, all train types, and complete office and wayside subsystems. Fully design and install PTC on pilot segments, test, and demonstrate performance, safety, reliability, and availability goals are all met.
- Define all interfaces with existing railroad systems including signal system, ATC, backbone

Success Criteria: Reliable Host/Tenant Integration

In order to integrate PTC into the existing railroad operation it is necessary to ensure the continued and safe operation of tenant railroads. Success is measured through agreements with tenants as operating partners and safe and continuous operation across railroad boundaries with PTC.

- Strategy for Temporal Separation: scheduling of time periods between host PTC railroad and non-ACSES railroad operating on shared track. Reliable strategy for protecting against violation by PTC equipped trains (i.e. zero speed restrictions during tenant periods)
- ACSES Railroad to ACSES Railroad Interoperability:
  - Secure communication
  - Consistent Messages and Protocol
  - Definition of both sides of boundary (overlap territory) within each ACSES system

Success Criteria: FRA System Safety Certification

The PTCSP is required for FRA approval prior to acceptance of the railroad PTC for revenue operation. This is at the completion of the Production stage before start of the Utilization and Support stages. Planning for certification and collection of evidence during implementation must be identified during the concept stage not at the end when it is submitted. Success is measured by FRA Type Approval and Certification of Safety of the railroad ACSES II PTC.

- Railroad System Safety Plan: require analyses and safety evidence to be collected during implementation early in the development by the PTC integrator and/or contractor
- Reliability and Availability Program: require allocation and calculation at each milestone,

fixed demonstration test at completion of Production stage

- Safety Verification of PTC
- FRACAS: include all reliability, availability, maintainability, and safety relevant incidents

Success Criteria: Commissioning All Segments

Commissioning and acceptance of the initial pilot segment results in FRA approval for the PTC system and includes demonstrating that all safety and performance goals have been met. Success is measured for each the complete PTC when the final segment is successfully tested, performance and safety goals are demonstrated to be maintained, and the railroad operates safe service with no adverse impacts.

- Segment Implementation Plan: priority sequence based on complexity and density of operation
- Vital Database: a single definition of the railroad must be translated and controlled through vital data for all PTC subsystems.
    - Tools for maintaining PTC vital databases controlled and managed through Configuration and Control Management Tools
    - Integrated interface for definition of railroad topology, PTC device identification, PTC configuration translated for each vital database
- Change Management: failures or anomalies identified during later segments must be regressed through earlier segments
    - Variances to approved segments reported to the FRA
    - Regression testing or redesign
- Complete Test and Commissioning Program including test tools

Success Criteria: Completion by FRA Deadline

In order to ensure that the mandated deadline of Dec. 31, 2015 is met for full PTC implementation, risk must be managed and mitigated during each stage of development to avoid delays to schedule. Success is measured through receipt of FRA approval for PTC completion by the deadline.

- Risk Management Plan
- Failure Review Board: include representatives of the railroad, Systems Integrator, and contractors to review all failures (under FRACAS) and agree on corrective actions
- Change Control Board: all changes reviewed and approved prior to implementation including regression
- Safety Certification Board: review all safety issues, assess impact to PTC, assess impact to signal system, agree on mitigation (design first)

Success Criteria: Training Of Operators & Maintainers

Delivery of a PTC System that meets all functional requirements by a Systems Integrator or Contractor is alone not enough for project completion. The means to train railroad personnel to operate the railroad and maintain the PTC for the life of the system must be in place. Initial operating and maintenance staff must be trained to support the earliest segments (pilot) using the delivered training program. Maintaining staff proficiency requires trained 'trainers' under the same training program. Success is measured when all trainees are proficient in the operation and maintenance of the system and trainers are proficient in the instruction of personnel.

- Training Materials: course materials, instructors, and training aids
- Full Curriculum: operations and maintenance under normal and abnormal conditions
- Train the Trainer Program
- Operations and Maintenance Manuals
- Maintenance Tools

Success Criteria: Managed Configuration

Once the complete PTC implementation is accepted and approved, the railroad begins to operate full PTC revenue service. As the railroad infrastructure changes the ability to modify PTC and continue operation is necessary. The life of the PTC extends for decades, well beyond any warranty period with the original suppliers, therefore accurate documentation and tools are necessary to support system changes. The ability to manage configuration changes while maintaining the integrity of operation, reliable performance, and safety is imperative. Success is measured through demonstration of

configuration change without performance or safety impact or degradation.

- PTC Product Vendor List (PTCPVL): Maintain and continuously update list of all PTC components within the railroad including version and contact information
- Configuration Management System: integrated tools for managing and changing vital databases, parameters, and configuration data
    - Complete development and as-built documentation
    - Change Notification: Process for notifying FRA and other user railroads of product design (PTCPVL) changes, especially due to failure or error
- Operations and Maintenance Manuals: Step by Step Instructions and Illustrations
- Complete training program including Train the Trainer curriculum

SUMMARY

Meeting the implementation of a Positive Train Control System by December 31, 2015 as mandated by 49CFR236I is indeed a challenge. Implementing a complex vital system as an overlay to an operating vital system however raises the bar of complexity. Missing any one success criterion may result in not completing by the mandated deadlines; overrun of budgets; failure to deliver all PTC functionality or major compromises to requirements; negative impact to service delivery including train delay; or worst case, impact to the safety of the overall signal system.

Using Systems Engineering principles and standards to guide the development of the specification for acquiring the PTC system increases the probability that all success criteria will be met. Conventional engineering and project management alone cannot be relied on to deliver a safe and fully functional PTC. What the Systems Engineer brings, as defined by the INCOSE SEgbk, is a focus 'on defining customer needs and required functionality early in the development cycle, documenting requirements, and then proceeding with design synthesis and system validation while considering the complete problem: operations, cost and schedule, performance, training and support, test, manufacturing, and disposal. SE considers both the business and the technical needs of all customers with the goal of providing a quality product that meets the user needs.'