RAIL SAFETY PROGRAM PLAN

for

SAFETY CRITICAL SYSTEMS

New York City Transit

System Safety Certification Board

Revision 0.0

January 24, 2017

Rail Safety Program Plan

Revision History

Revision	Date	Description
0.0	1/24/2017	Initial draft

NYCT SSCB APPROVALS

RAIL SAFETY PROGRAM PLAN

New York City Transit

_____ _____ Nidhish Patel, P.E. Date SSCB Chair Program Executive, Signals & Train Control Capital Program Management	_____ _____ Kenneth Brown Date SSCB Member Director, Risk Assessment and Fire Safety Department of Subways
_____ _____ Paul Camera Date SSCB Member Chief Electrical Officer Department of Subways, Power and Signals	_____ _____ Kenneth Mooney, P.E. Date SSCB Member Chief Engineering Officer Department of Subways, Engineering
_____ _____ Chan Samsundar Date SSCB Member Transit Applications Technology Information Services	_____ _____ Joseph Bromfield Date SSCB Member Vice President & Chief Mechanical Officer Division of Car Equipment
_____ _____ Tony Abdallah Date SSCB Member Chief Transportation Officer Rapid Transit Operations	_____ _____ Chandra Patel, P.E. Date SSCB Member Chief, Signals Engineering Engineering Services, Capital Program Management
_____ _____ Robert Gomez, P.E. Date SSCB Member Program Officer Signals & Train Control Capital Program Management	

Contents

ABSTRACT

This Rail Safety Program Plan (RSPP) has been created to ensure all such safety critical systems comply with applicable US safety standards and accepted industry practice including the requirements of the Federal Railroad Administration Rulemaking 49 CFR Part 236 Subpart H. It applies to all Solid State Interlocking (SSI) and Communication Based Train Control (CBTC) systems for all New York City Transit (NYCT) projects deploying these systems. The plan shall be considered a "living" document and is subject to change in accordance with direction provided by the NYCT System Safety Certification Board (SSCB).

1 INTRODUCTION, GOALS AND OVERVIEW

1.1 Introduction

This Railroad Safety Program Plan (RSPP) is NYCT SSCB's strategic safety planning document for the development and deployment of safety critical processor based signal and train control systems; specifically, Solid State Interlocking (SSI) , Communications Based Train Control (CBTC) and Cab Signal Systems.

While there are no US regulations that define a required safety process for signal systems in heavy-rail transit applications, this RSPP has been developed to be consistent with applicable US safety standards and accepted industry practice including the requirements of the Federal Railroad Administration Rulemaking 49 CFR Part 236 Subpart H, *Standards for Processor Based Signal and Train Control Systems*, Federal Register, March 7, 2005; referred to as *Subpart H* further in this document. Refer to section 2.1 for a list of all standards.

This RSPP's subsequent sections identify the requirement documents for safety certification and the safety program plan. With these documents, NYCT's RSPP provides all requirements and concepts, verification and validation, human factors and configuration management employed by NYCT to meet safety goals for safety critical SSI, Cab Signal and CBTC systems. Further, it establishes the definitive requirements for the Contractor's Project Safety Plan (PSP) that must be prepared for the deployment, operation and maintenance of these systems. The PSP must be compliant with this RSPP and approved by NYCT.

1.2 Goals and Objectives

The overall goals for the deployment of any safety-critical processor based signal and train control system are to enhance the safety and/or increase capacity and efficiency where the system is deployed. The objective of this RSPP is to ensure the deployment of such systems is guided by the provisions of Subpart H and other US safety standards and practices.

This RSPP will provide a uniform set of requirements for developing and implementation a system safety program.

1.3 Document Overview

Following this introduction, this RSPP document contains the following sections:

- Paragraph 2 defines the standards referred to and acronyms used in the RSPP documents
- Paragraph 3 defines NYCT responsibility and provides the NYCT Rail Safety Program Plan Requirements. It identifies the key NYCT and Contractor documents.

2 APPLICABLE DOCUMENTS AND TERMS USED

2.1 Documents

Following are the Codes, standards and specifications referenced in this RSPP.

1. 1474.1-2004, IEEE Standard for Communication Based Train Control Performance Requirements and Functional Requirements.
2. 1228-1994, IEEE Standard for Software Safety Plans.
3. MIL-STD-882C System Safety Program Requirements, 19 January 1993.
4. 1483-2000, IEEE Standard for Verification of Vital Functions in Processor-Based Systems.
5. CENELEC Standard Publication EN 50126:1999: Railway applications. The specification and demonstration of reliability, availability, maintainability and safety (RAMS).
6. CENELEC Standard Publication EN 50128:2011: Railway applications - Communication, signaling and processing systems - Software for railway control and protection systems. March 2001.
7. CENELEC Standard Publication EN 50129:2003: Railway applications. Communication, signaling and processing systems. Safety related electronic systems for signaling.
8. Federal Transit Administration Handbook for Safety and Security Certification. FTA-MA-90-5006-02-01. November 2002.
9. Nuclear Regulatory Commission Fault Tree Handbook NUREG-0492. January 1981.
10. IEC 61820 Analysis techniques for system reliability – Procedure for failure mode and effects analysis (FMEA). IEC 60812:2006.
11. IEEE 1483-2000, Standard for Verification of Vital Functions in Processor-Based Systems Used in Rail Transit Control, March 30, 2000
12. US FRA Railroad Safety Advisory Committee (RSAC) Notice of Proposed Rulemaking (NPRM), CFR 49, Part 236, Subpart H, Safety of Processor Based Train Control Systems, Federal Register (August 10, 2001)
13. Federal Railroad Administration (FRA) 49 CFR Part 236 Subpart H, Standards for Processor Based Signal and Train Control Systems, Federal Register, March 7, 2005
14. Federal Railroad Administration (FRA) Hazard Analysis Guidelines for Transit Projects, DOT-FTA-MA-26-5005-00-01, January 2000
15. Handbook for Transit Safety and Security Certification, FTA-MA-90-5006-02-01, Final Report, November 2002
16. IEEE 12207.0, Standard for Information Technology – Software Life Cycle Processes, May 27, 1998
17. IEEE 1012-2012, Standard for Software Verification and Validation, May 25, 2012
18. American Railway Engineering and Maintenance of Way Association (AREMA) Signal and Communication Manuals of Recommended Practices, 2012
19. MIL-STD-498, Software Development and Documentation, December 5, 1994.

2.2 Acronyms

Key abbreviations and acronyms utilized in this plan are defined below, followed by definitions of key terminology:

AREMA – American Railway Engineering and Maintenance of Way Association

CBTC – Communications Based Train Control

CPM – Capital Program Management

CPM/VSI - Capital Program Management/ Vital Systems Integrity

FRA – Federal Railroad Administration

NYCT – New York City Transit

PSP – Project Safety Plan

SSCB – System Safety Certification Board

SSCP – System Safety Certification Plan

SSI – Solid State Interlocking

SSPP – System Safety Program Plan

VSI – Vital Systems Integrity

3.0 NYCT RAIL SAFETY PROGRAM PLAN REQUIREMENTS

This document, the NYCT SSCB Rail Safety Program Plan (RSPP), and the documents identified in the table below as Sections of this document comprise the principle safety documents for all safety-critical SSI and CBTC systems implemented. Their intent is to ensure that safety and the defined safety requirements are an inherent part of the project. For all projects, compliance is fulfilled through the execution of activities identified in the following documents:

SECTION	TITLE	DESCRIPTION
Wrapper Document	NYCT SSCB Rail Safety Program Plan (RSPP)	This document
1.	System Safety Program Plans for CBTC and SSI systems	Section 1 contains the System Safety Program Plans (SSPPs) for the CBTC and SSI systems. These System Safety Program Plans are analogous to the Product Safety Plan as defined by the FRA 49 CFR 236 subpart H. These System Safety Program Plans (SSPP) have been created to specify the minimum Project Safety Plans (PSP) requirements for Communication Based Train Control (CBTC) and Solid Sate Interlocking (SSI) systems for all New York City Transit (NYCT) projects deploying these systems.
1.1	NYCT System Safety Program Plan – SSI (SSPP):	Subsection 1.1 specifies the minimum Project Safety Plan (PSP) requirements to ensure the SSI system to be deployed complies with the regulatory requirements and undergoes the necessary analyses for such a safety-critical system. The document contained in 1.1 is section 17JC-A of the SSI Contract Specification document and is the System Safety Program Plan for all SSI projects.
1.2	NYCT System Safety Program Plan – CBTC (SSPP):	Subsection 1.2 specifies the minimum Project Safety Plan (PSP) requirements to ensure the CBTC system to be deployed complies with the regulatory requirements and undergoes the necessary analyses for such a safety-critical system. The document contained in 1.2 is section 24M of the CBTC Contract Specification document and the System Safety Program Plan for all CBTC projects.

SECTION	TITLE	DESCRIPTION
1.3	NYCT System Safety Program Plan – Cab Signal (SSPP):	Subsection 1.3 specifies the minimum Project Safety Plan (PSP) requirements to ensure the Cab Signal system to be deployed complies with the regulatory requirements and undergoes the necessary analyses for such a safety-critical system. The document contained in 1.3 is section 24M of the Cab Signal Contract Specification document and the System Safety Program Plan for all Cab Signal projects.
2.	NYCT System Safety Certification Plan (SSCP)	Section 2 contains the System Safety Certification Plans for the CBTC/SSI systems and the Wayside Devices. These System Safety Certification Plans (SSCPs) have been created to document the safety certification process for Solid State Interlocking (SSI), Communication Based Train Control (CBTC) and Wayside Device systems for all New York City Transit (NYCT) projects deploying these systems.
2.1	System Safety Certification Plan (SSCP) for CBTC, Cab Signal and SSI systems.	Subsection 2.1 contains the System Safety Certification Plan (SSCP) which defines the process by which the SSI, Cab Signal and CBTC Systems will be certified as being safe to operate in revenue service. The document contained in subsection 2.1identifies the certification process for all SSI and CBTC projects.
2.2	System Safety Certification Plan (SSCP) for Wayside Devices.	Subsection 2.2 contains the System Safety Certification Plan (SSCP) for Wayside Devices. This System Safety Certification Plan (SSCP) has been created to document the safety certification process for Wayside signaling products selected by the NYCT SSCB prior to their deployment to revenue service.

The System Contractor has fundamental responsibility for safety of the complete System, and has a safety assurance process that is directed to meeting the safety requirements defined in the subject contract for the System. That process, defined in the Contractor's Project Safety Plan, involves activities directed to designing safety into the System and demonstrating safety via the conduct of hazard and safety analyses, inspections, testing and the conduct of a quantitative risk assessment on the system.

Overall safety certification of the System It is the responsibility of NYCT- Capital Program Management (CPM) in conjunction with the System Safety Certification Board (SSCB) to ensure the system design, implementation, operation and maintenance meets the requirements of this RSPP. Further, the CPM will provide final approvals of safety evidence pertaining to safety certifiable items of the system. Day-to-day management of the safety certification process is the responsibility of CPM's Vital Systems Integrity (CPM-VSI). The Contractor and all NYCT working groups and support organizations (e.g., Independent Safety Assessor, Technical Consultant) involved in the certification process are responsible to NYCT-CPM. From a safety standpoint, CPM, the Technical Consultant (TC), the Contractor, Working Groups (WG) and the ISA report to the SSCB.

Section 1 – SYSTEM SAFETY PROGRAM PLANS FOR SAFETY CRITICAL SYSTEMS (SSPPs)

Introduction – Section 1

This section contains the System Safety Program Plans for the CBTC and SSI systems. These System Safety Program Plans are analogous to the Product Safety Plan as defined by the FRA 49 CFR 236 subpart H. These System Safety Program Plans (SSPP) have been created to specify the minimum Project Safety Plans (PSP) requirements for Communication Based Train Control (CBTC) and Solid Sate Interlocking (SSI) systems for all New York City Transit (NYCT) projects deploying these systems.

Section 1.1 contains the System Safety Program Plan for CBTC systems.

Section 1.2 contains the System Safety Program Plan for SSI systems.

Section 1.3 contains the System Safety Program Plan for Cab Signal systems.

Note: These are contract-specific sections and the actual supplier contracts will be based on these sections, depending on system type. The contract sections may include minor modifications to address contract-specific characteristics.

Section 1.1

Section 1.1 contains the System Safety Program Plan for CBTC systems.

Section 1.2

Section 1.2 contains the System Safety Program Plan for SSI systems.

Section 1.3

Section 1.3 contains the System Safety Program Plan for Cab Signal systems.

Section 2 – SYSTEM SAFETY CERTIFICATION PLANS FOR SAFETY CRITICAL SYSTEMS (SSCPs)

Introduction – Section 2

This section contains the System Safety Certification Plans for the CBTC/SSI/Cab Signal systems and the Wayside Devices. These System Safety Certification Plans (SSCP) have been created to document the safety certification process for Solid State Interlocking (SSI), Communication Based Train Control (CBTC) and Wayside Device systems for all New York City Transit (NYCT) projects deploying these systems.

Section 2.1 contains the System Safety Certification Plan for CBTC, Cab Signal and SSI systems.

Section 2.2 contains the System Safety Certification Plan for Wayside Devices.

Note: These sections are standard for all CBTC, Cab Signal, SSI, and Wayside Device NYCT system acquisitions, and shall be applied to all such projects.

Section 2.1

Section 2.1 contains the System Safety Certification Plan for CBTC, Cab Signal and SSI systems.

Section 2.2

Section 2.2 contains the System Safety Certification Plan for Wayside Devices.