35. Standard for Vital Processor-Based System Inspection, Testing and Configuration Control

Approved January 10, 2003
APTA Rail Transit Standards Fixed Structures Inspection and Maintenance Committee

Approved September 28, 2003
APTA Rail Transit Standards Task Force

Authorized January 28, 2004
APTA Rail Transit Standards Policy Committee

Abstract: This standard provides procedures for the inspection, testing, and configuration control of rail transit vital processor-based systems.

Keywords: configuration control, firmware, inspection, interlocking, microprocessor, software, signal, test, testing, vital processor

---

Introduction

(This introduction is not a part of APTA RT-SC-S-035-03, *Standard for Vital Processor-Based System Inspection, Testing and Configuration Control*.)

APTA rail transit safety standards represent an industry consensus on safety practices for rail transit systems to help achieve a high level of safety for passengers, employees, and the general public. This document was created by and for those parties concerned with its provisions; namely, rail transit systems (operating agencies), manufacturers, consultants, engineers, and general interest groups. This standard provides procedures for rail transit vital processor-based system inspection, testing, and configuration control.

APTA recommends this standard for:

- Individuals or organizations that inspect, maintain, and/or operate rail transit systems
- Individuals or organizations that contract with others for the inspection, maintenance, and/or operation of rail transit systems
- Individuals or organizations that influence how rail transit systems are inspected, maintained, and/or operated (including but not limited to consultants, designers, and contractors)

This standard intends to meet the following objectives:

- To ensure special life/safety equipment is operational and reliable
- To help rail transit systems incorporate safety considerations during the inspection and maintenance process
- To identify inspection criteria and maintenance standards that provide a high level of passenger and personnel safety

The application of any standards, practices, or guidelines contained herein is voluntary. In some cases, federal and/or state regulations govern portions of how a rail transit system operates. In such cases, the government regulations override any conflicting practices this document requires or recommends.

Participants

APTA greatly appreciates the contributions of the following members of the Signals and Communications Subcommittee who provided the primary effort in drafting the *Standard for Vital Processor-Based System Inspection, Testing and Configuration Control*:

Carlton "Don" Allen, P.E.
Sal Arceo
Gabrielle Bayme
Paul Camera
Lenny De Meyer
Michael Esford
Patrick Lavin
Ruben Madrigal
Thomas Peacock
Stephen Roberts
Carey Vaughn

The following members of the Rail Transit Standards Fixed Structures Inspection and Maintenance Committee contributed to the review and approval process of the *Standard for Vital Processor-Based System Inspection, Testing and Configuration Control*:

James Dwyer, *Chair*
Frank Cihak, *Vice Chair*

Anthony Adams
Carlton "Don" Allen, P.E.
Sal Arceo
Roger Avery
Peter Bertozzi
Steven Bezner, P.E.
Raymond Borge
Michael Brown
John Bumanis
Clay Bunting
R. Sean Burgess
Paul Camera
David Cappa, P.E.
Gricelda Cespedes
Robert Chappell
Frank Cihak
Catherine Cronin
Lenny De Meyer
Tom Devenny
David Dunderdale
James Dunn
James Dwyer
William Early, P.E.
Percy Erves
Michael Esford
Richard Falcon
Ray Favetti
Peter Fedun, P.E.
Steve Feil
Robert Fiore
John Gaito
Ricky Green
Mohammad Irshad
Patrick Lavin
Harry Lupia
Frank Machara
Ruben Madrigal
Michael Monastero
Bill Petit
David Rankin
Pingali Rao, P.E.
Richard Raschke
James Redding
Stephen Roberts
Charles Slavis, P.E.
Frederick Smith, P.E.
Richard Spatz
Charles Stanford
F. Brian Steets
Paul Swanson, P.E.
Steven Thompson
Fred Tijan
Gary Touryan
Carey Vaughn
James Wang, P.E.

APTA Rail Transit Standards Fixed Structures Inspection and Maintenance Committee project consultants:

Peter Gentle, P.E., *STV Incorporated*
Carol Rose, *STV Incorporated*

APTA Rail Transit Standards project team:

Gabrielle Bayme, *Standards Development Program Specialist and Project Editor*
Saahir Brewington, *Administrative Assistant and Project Editor*
Antoinette Hankins, *Program Assistant*
Thomas Peacock, *Director-Operations & Technical Services*
David Phelps, *Senior Project Manager - Rail Programs*

Contents

Standard for Vital Processor-Based System Inspection, Testing and Configuration Control

1. Overview

1.1 Scope

This document establishes standard requirements for the inspection, testing, and configuration control of vital processor-based interlocking and signal systems. This document only addresses vital processor system components. Conventional equipment based portions of vital processor-based signal systems shall be governed by the applicable standards. Non-vital processor equipment shall be governed by *APTA RT-RP-SC-030-003, Recommended Practice for Non-Vital Processor-based Systems Inspection, Testing and Configuration Control.*[1]

1.2 Purpose

The purpose of this standard is to verify that vital processor-based systems are operating safely and as designed through periodic inspection, testing, and configuration control, thereby increasing reliability and reducing the risk of hazards and failures.

1.3 Alternate practices

Individual rail transit systems may modify the practices in this standard to accommodate their specific equipment and mode of operation. APTA recognizes that some rail transit systems may have unique operating environments that make strict compliance with every provision of this standard impossible. As a result, certain rail transit systems may need to implement the standards and practices herein in ways that are more or less restrictive than this document prescribes. A rail transit system (RTS) may develop alternates to the APTA standards so long as the alternates are based on a safe operating history and are described and documented in the system's safety program plan (or another document that is referenced in the system safety program plan).

Documentation of alternate practices shall:

a) Identify the specific APTA rail transit safety standard requirements that cannot be met

b) State why each of these requirements cannot be met

c) Describe the alternate methods used

[1] For references in italics, see Section 2.

d) Describe and substantiate how the alternate methods do not compromise safety and provide a level of safety equivalent to the practices in the APTA safety standard (operating histories or hazard analysis findings may be used to substantiate this claim).

2. References

This document shall be used in conjunction with the most recent version of the following documents.

APTA RT-RP-SC-030-003, Recommended Practice for Non-Vital Processor-based Systems Inspection, Testing and Configuration Control.

3. Definitions and acronyms

For the purposes of this standard, the following definitions and acronyms apply:

3.1 Definitions

2.1.1 application software: Software that defines the site-specific functions of a system, e.g., route locking.

2.1.2 check sum: A number derived from a cyclic redundancy check used to verify accuracy of data.

2.1.3 cyclic redundancy check (CRC): An algorithmic inspection of the data content of firmware.

2.1.4 executive software: Software that performs the basic operations of a system, e.g., memory mapping, addressing, self-diagnostics, etc. Typically of standard format that does not change from installation to installation.

2.1.5 firmware: A device that is programmed with instruction set software and installed in a processor-based system, e.g., electronic programmable read only memory (EPROM).

2.1.6 hazard: Any real or potential condition that can cause injury, death, or damage or loss of equipment or property.

2.1.7 interlocking: An arrangement of signals and signal appliances so interconnected that their movements must succeed each other in proper sequence and for which interlocking rules are in effect. It may be operated manually or automatically.

2.1.8 non-vital system: Any system, the function of which does not affect the safety of train operation.

2.1.9 operations control center (OCC): That facility from which train control, train dispatching, and/or train supervision takes place for the entire RTS or for specific segments of a system if there is more than one control center. *Syn:* **rail control center, rail operations center, rail service control center, train command center.**

2.1.10 original equipment manufacturer (OEM): The enterprise that initially designs and builds a piece of equipment.

2.1.11 personal protective equipment (PPE): All clothing and other work accessories designed to create a barrier against workplace hazards. Examples include safety goggles, blast shields, hard hats, hearing protectors, gloves, respirators, aprons, and work boots.

2.1.12 processor-based: A system dependent upon a digital processor for proper functioning.

2.1.13 rail transit system (RTS): The organization or portion of an organization that operates rail transit service and related activities. *Syn:* **operating agency, operating authority, transit agency, transit authority, transit system**.

2.1.14 signal: An appliance that conveys information governing train movement.

2.1.15 vital system: Any system, the function of which affects the safety of train operations.

3.2 Acronyms

OCC	operations control center
OEM	original equipment manufacturer
PPE	personal protective equipment
RTS	rail transit system

4. Inspection, testing and configuration control requirements

4.1 Inspection, testing and configuration control frequency

The inspection and testing procedures in this standard shall be performed when vital processor-based systems are placed in service, when they are modified, repaired, or disarranged, or as otherwise deemed necessary by the RTS. Configuration control shall be maintained at all times.

The RTS shall determine the need for additional inspection and testing frequencies for vital processor-based systems. A review of the following factors may be useful in making this assessment:

- OEM-recommended intervals
- Industry experience
- Operating environment/conditions
- Historical data
- Reliability-centered maintenance program development
- Failure analysis
- RTS testing and experience

– Regulatory requirements

The frequency of tasks shall comply with applicable federal, state, and local regulations.

4.2 Training

The RTS and/or their maintenance contractors shall develop and execute training programs that provide employees with the knowledge and skills necessary to safely and effectively perform the tasks outlined in this standard.

4.3 Materials

No consumable materials are required for vital processor inspection, testing, and configuration control unless otherwise specified by the OEM and/or RTS.

4.4 Tools

The following tools are required for the inspection, testing, and configuration control of vital processor-based systems:

– Firmware extraction and insertion tool

– Electrostatic discharge protection equipment

– RTS-approved portable radio

– Standard tools carried by maintenance personnel

– Additional tools as required by the OEM and/or RTS

* Calibrate in accordance with OEM and/or RTS requirements.

4.5 Personal protective equipment

Personal protective equipment, as required by the RTS, shall be worn at all times during inspection and testing.

4.6 Safety

RTS safety rules, procedures, and practices shall be followed at all times during inspection and testing.

4.7 Inspection, testing and configuration control procedures

Vital processor system inspection, testing and configuration control procedures may be modified for each rail transit system's requirements (see Section 1.3) but shall contain the steps listed in Sections 4.7.1-4.7.3 as a minimum.

4.7.1 Inspection

4.7.1.1 Notify the operations control center (OCC) and/or other authorities of the inspection activities to be performed.

4.7.1.2 Inspect area for debris, water, or any other conditions that could adversely affect the safe operation of the equipment.

4.7.1.3 Follow RTS electro-static discharge protection procedures to prevent damage to the equipment.

4.7.1.4 Inspect equipment for physical damage, frayed or loose wiring, plugs and connectors are properly secured, loose or missing hardware, and proper insertion of printed circuit cards and components.

4.7.1.5 Measure power supplies and power sources for proper values and tolerances.

4.7.1.6 Inspect equipment for active error codes and observe system status lights for proper system operation.

4.7.1.7 Verify firmware in operation and any on-site spare firmware revisions are consistent with configuration control documentation.

4.7.1.8 Perform system functional testing as deemed necessary to verify proper and safe system operation.

4.7.1.9 Ensure covers and locks are in place and secured.

4.7.1.10 Notify the OCC and/or other authorities when inspection is complete.

4.7.2 Testing

4.7.2.1 Notify the OCC and/or other authorities of the testing activities to be performed.

4.7.2.2 Test all physical wiring and/or wiring changes.

4.7.2.3 Perform testing using a RTS-approved procedure that ensures safe operation of all interlocking and signal system functions.

4.7.2.4 Perform testing under simulated conditions utilizing the approved procedure to ensure safe operation prior to executing operational testing.

4.7.2.5 If applicable, simulate failure of primary system and verify operation of back up systems.

4.7.2.6 Return system to normal mode of operation.

4.7.2.7 Perform configuration control procedures. See Section 3.7.3.

4.7.2.8 Notify the OCC and/or other authorities when testing is complete.

4.7.3 Configuration control

4.7.3.1 Notify the OCC and/or other authorities of the configuration control activities to be performed.

4.7.3.2 Identify the current software version in use for each vital processor-based system including the date placed in service, name, revision level, revision date, and check sum value.

4.7.3.3 Software shall be archived and placed in configuration control to facilitate firmware programming if required and to facilitate control for future revision.

4.7.3.4 Firmware shall be labeled with name, revision level, revision date, check sum value, and socket location on printed circuit card, e.g. U32.

4.7.3.5 Only current versions of firmware shall be stored in signal equipment rooms.

4.7.3.6 Hardware configuration such as the position of field settable switches, jumpers, board address assignments, keying, and proper revision levels shall be documented and maintained on site.

4.7.3.7 Notify the OCC and/or other authorities when configuration control activities are complete.

4.8 Correction of deficiencies

Deficiencies identified during vital processor-based system inspection, testing, and configuration control shall be corrected and documented in accordance with OEM and/or RTS requirements.

4.9 Documentation

Inspection, testing, and configuration control activities shall be documented, reviewed, and filed in accordance with RTS procedures.

Annex A

(informative)

Bibliography

[B1] 49 CFR Part 209, Standards for Development and Use of Vital processor-Based Signal and Train Control Systems; Proposed Rule, August 10, 2001.

[B2] American Railway Engineering and Maintenance of Way Association Signal Manual.

[B3] Original equipment manufacturer (OEM) specifications for vital processor-based system inspection, testing, and configuration control.

[B4] Rail transit system (RTS) procedures for vital processor-based system inspection, testing, and configuration control.

[B5] South Eastern Pennsylvania Transit Authority, Standard Instructions Governing Construction and Maintenance of Wayside Signal Systems.