30. Recommended Practice for Non-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 recommended practice provides guidelines for the inspection, testing, and configuration control of rail transit non-vital processor-based systems.

Keywords: configuration control, firmware, microprocessor, non-vital processor, signal, software

---

Copyright © 2004 by The American Public Transportation Association
1666 K Street, NW, Washington, DC, 20006-1215, USA

No part of this publication may be reproduced in any form, in an electronic retrieval system or otherwise, without the prior written permission of The American Public Transportation Association.

Introduction

(This introduction is not a part of APTA RT-SC-RP-030-03, *Recommended Practice for Non-Vital Processor-Based System Inspection, Testing and Configuration Control*.)

APTA rail transit safety standards and recommended practice represent an industry consensus on 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 recommended practice provides guidelines for inspecting and testing rail transit non-vital processor-based systems.

APTA recommends this practice 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)

The application of any 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 recommends.

Copyright © 2004 APTA. All rights reserved.

Participants

APTA greatly appreciates the contributions of the following members of the Signals and Communications Subcommittee who provided the primary effort in drafting the *Recommended Practice for Non-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 *Recommended Practice for Non-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*

Copyright © 2004 APTA. All rights reserved.

Contents

1. Overview 30.1

1.1 Scope 30.1
1.2 Purpose 30.1

2. References 30.1

3. Definitions and acronyms 30.1

3.1 Definitions 30.1
3.2 Acronyms 30.2

4. Inspection, testing and configuration control provisions 30.2

4.1 Inspection, testing, and configuration control frequency 30.2
4.2 Training 30.3
4.3 Materials 30.3
4.4 Tools 30.3
4.5 Personal protective equipment 30.4
4.6 Safety 30.4
4.7 Inspection, testing and configuration control procedures 30.4
4.7.1 Inspection 30.4
4.7.2 Testing 30.5
4.7.3 Configuration control 30.5
4.8 Correction of deficiencies 30.5
4.9 Documentation 30.6

Annex A (informative) Bibliography 30.7

Copyright © 2004 APTA. All rights reserved.

Recommended Practice for Non-Vital Processor Based Systems Inspection, Testing and Configuration Control

1. Overview

1.1 Scope

This document establishes recommended guidelines for the inspection, testing, and configuration control of non-vital processor based systems. This document only addresses non-vital processor system components. Conventional equipment based portions of non-vital processor based systems should be governed by the applicable recommended practices. Vital processor equipment shall be governed by *APTA RT-RP-SC-035-003, Recommended Practice for Vital Processor-Based Systems Inspection, Testing, and Configuration Control.*[1]

1.2 Purpose

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

2. References

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

APTA RT-RP-SC-035-003, Recommended Practice for Vital Processor-Based Systems Inspection, Testing, and Configuration Control.

3. Definitions and acronyms

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

3.1 Definitions

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

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

Copyright © 2004 APTA. All rights reserved.

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

3.1.3 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).

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

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

3.1.6 operations control center (OCC): A location or locations designed, equipped, and staffed for the purposes of monitoring and controlling RTS activities from a central location or locations. *Syn:* **rail control center, rail operations center, rail service control center.**

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

3.1.8 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.

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

3.1.10 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**.

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

3.2 Acronyms

DMM	digital multi-meter
OCC	operations control center
OEM	original equipment manufacturer
PPE	personal protective equipment
RTS	rail transit system

4. Inspection, testing and configuration control provisions

4.1 Inspection, testing, and configuration control frequency

The inspection and testing procedures in this recommended practice should be performed when non-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 should be maintained at all times.

Copyright © 2004 APTA. All rights reserved.

The RTS should determine the need for additional inspection, testing, and configuration control frequencies for non-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 should comply with applicable federal, state, and local regulations.

4.2 Training

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

4.3 Materials

No consumable materials are recommended for inspecting and testing non-vital processor systems unless otherwise specified by the OEM and/or RTS.

4.4 Tools

The following tools are recommended for inspecting and testing non-vital processor-based systems:

- Firmware extraction and insertion tool
- Electrostatic discharge protection equipment
- RTS-approved portable radio
- Standard tools carried by maintenance personnel

Copyright © 2004 APTA. All rights reserved.

– 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, should 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

The inspection, testing, and configuration control procedures in this recommended practice may be modified for each rail transit system's requirements but should 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 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 system operation.

4.7.1.9 Ensure covers and locks are in place and secured.

Copyright © 2004 APTA. All rights reserved.

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 proper operation of all system functions.

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

4.7.2.5 Return system to normal mode of operation.

4.7.2.6 Perform configuration control procedures. See Section 3.7.3.

4.7.2.7 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 non-vital processor based system including the date placed in service, name, revision level, revision date, and checksum value.

4.7.3.3 Archive and place software under configuration control.

4.7.3.4 Label firmware with name, revision level, revision date, checksum value, and socket location on printed circuit card, for example, a U32.

4.7.3.5 Store only current versions of firmware in signal equipment rooms. Another current version of firmware may be stored off site.

4.7.3.6 Document and maintain hardware configuration such as the position of field settable switches, jumpers, board address assignments, keying, and proper revision levels on site.

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

4.8 Correction of deficiencies

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

Copyright © 2004 APTA. All rights reserved.

4.9 Documentation

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

Copyright © 2004 APTA. All rights reserved.

Annex A

(informative)

Bibliography

[B1] American Railway Engineering and Maintenance of Way Association Signal Manual.

[B2] Original equipment manufacturer (OEM) specifications for non-vital processor-based system inspection, testing and configuration control.

[B3] Rail transit system (RTS) procedures for non-vital processor-based system inspection, testing and configuration control.

[B4] South Eastern Pennsylvania Transit Authority, Standard Instructions Governing Construction and Maintenance of Wayside Signal Systems.

Copyright © 2004 APTA. All rights reserved.