TITLE:
Automatic Train Control (ATC) Update

PRESENTATION SUMMARY:
Provide an overview of the completed Automatic Train Control System Safety Analysis (SSA).

PURPOSE:
The purpose of this presentation is to provide the Committee a briefing on findings, recommendations, remedial actions and plan for closure of the National Transportation Safety Board (NTSB) recommendation on the ATC System Safety Analysis.

DESCRIPTION:
After the June 22, 2009 Washington Metro train collision near Fort Totten station, the NTSB made the following recommendations (dated July 27, 2010):

- R-10-12: Conduct a comprehensive safety analysis of the Metrorail automatic train control system to evaluate all foreseeable failures of this system that could result in a loss of train separation, and work with your train control equipment manufacturers to address in that analysis all potential failure modes that could cause a loss of train detection, including parasitic oscillation, cable faults and placement, and corrugated rail.
- R-10-13: Based on the findings of the safety analysis recommended in R-10-12, incorporate the design, operational, and maintenance controls necessary to address potential failures in the automatic train control system.

Metro contracted an independent consultant to perform a safety analysis of the automatic train control system to address the NTSB recommendations.

The ATC Safety Analysis' primary focus is the wayside audio frequency track circuit system and the carborne ATC system with hazard analysis of the operating and support functions as well as specific components level subsystem analysis. The primary analysis findings can be categorized in two major classes:

- Process – Addressed with updated preventative maintenance and testing guidelines, standard specifications and operating procedures
- Gaps between the failure mode effects analysis in the original product safety case during the period of manufacture and the modern safety case requirements of today. Closure of
The findings has been accomplished through various methods of update to safety cases, review of service history and replacement or upgrade to equipment.

This independent review was initiated in 2010 and all analysis has been concluded. A final draft of the application safety case has been provided to Metro for review and upon completion will be provided to the NTSB for closure of the recommendation.

**Key Highlights:**

- The Automatic Train Control System Safety Analysis has been completed and a closeout plan has been established for all findings and recommendations;
- The final application safety case report will be provided to the NTSB for review and closure;
- Identified hazards will be tracked and closed in the Hazard Log and System Implementation Gap Analysis Report (SIGAR) under the control of Metro; and
- Progress continues on programs for systems upgrades and replacements as well as update to process related findings.

**Background and History:**

The ATC network provides for the safe and efficient movement of trains through a series of track circuits and integrated logic for routing controls and speed controls. Major subcomponents of the ATC network include Automatic Train Operation (ATO) and Automatic Train Protection (ATP). ATO is a system that uses integrated logic between the wayside system where the train speeds and braking are regulated automatically without required intervention from the operator. ATP is the system that provides safe train separation through the same network but where the operator is in direct control of the train speed and braking. It should be noted that while the train is in “manual” control, the ATP is still active and any violation of speed command by the operator will cause the train to automatically reduce speed, thereby resulting in the safe separation of trains or automatic train protection. ATO is desirable because of the efficiency and consistency of accelerating and braking provided by the trains on-board ATC system. Therefore, Metro is taking a systematic and calculated approach to returning to ATO.

**Discussion:**

Metro has been undertaking major steps to return to Automatic Train Operation (ATO) for the safe and efficient movement of trains throughout the system. The major steps include:

- Addressing National Transportation Safety Board (NTSB) recommendations:
  - ATC System Safety Analysis
  - Replacement of Generation II Track Circuits
  - Track Circuit Monitoring Tool or Loss of Shunt detection
  - Development of test/maintenance procedure in ATC-1000, 2000 and 3000
- Deployment of the right equipment and tools
- Organizational changes
- Development and implementation of processes, equipment, and procedures
FUNDING IMPACT:

Information item only.

TIMELINE:

<table>
<thead>
<tr>
<th>Previous Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>March 11, 2010 - Presentation to the Customer Service and Operations Committee on &quot;Manual vs. Automatic Train Operation and Operational Restrictions&quot;</td>
</tr>
<tr>
<td>November 01, 2012 - Presentation to the Safety and Security Committee on &quot;Automatic Train Control (ATC) Update&quot;</td>
</tr>
<tr>
<td>June 13, 2013 - Presentation to the Safety and Security Committee on &quot;Automatic Train Control System Update&quot;</td>
</tr>
</tbody>
</table>

RECOMMENDATION:

No recommendation, information item only.
This page intentionally left blank.
Automatic Train Control (ATC) Update

Safety and Security Committee

April 24, 2014
Background

- Recommendations made by the National Transportation Safety Board (NTSB) – July 27, 2010:
  
  **R-10-012:** Perform System Safety Analysis (SSA) on ATC network
  
  **R-10-013:** Implement programs to resolve findings of R-10-12

- Contracted independent consultant to perform System Safety Analysis (SSA)
System Safety Analysis (SSA)

R-10-12: Perform System Safety Analysis on ATC network

“Conduct a comprehensive safety analysis of the Metrorail automatic train control system to evaluate all foreseeable failures of this system that could result in a loss of train separation . . .”
System Safety Analysis (SSA) Methodology:

- Preliminary Hazard Analysis (PHA)
- System Hazard Analysis (SHA)
- Interface Hazard Analysis (IHA)
- Operating & Support Hazard Analysis
- Subsystems Hazard Analysis:
  - Carborne Hazard Analysis
  - Wayside Hazard Analysis
- Hazard Log
- Recommendations
- System Implementation Gap Analysis Report (SIGAR)
- Safety Requirements
Preliminary Hazard Analysis and System Hazard Analysis

**PHA:** Initial identification of hazards presented in the current Automatic Train Control subsystem

**SHA:** Performed safety analysis of the interface portion of the equipment currently in use and evaluated foreseeable critical failures
Interface Hazard Analysis

IHA:

- Detailed safety review confined to specific portions of the Automatic Train Protection portion of the ATC subsystem.
- Elements not relevant to train safety not included.
O&SHA:

- Initial identification of hazards based upon actions of personnel or deficiencies in WMATA procedures.
- Verification on compliance of Metro maintenance procedures with the manufacturers requirements.
Failure Mode Effect Analysis (FMEA) Gaps

1980’s Failure Modes List

- Mitigated or Tolerable Hazards
- Potential Unknown Hazards (failure modes not analyzed)

Robust safety case section on “1980’s coverage”

Gap identification and “type of risk exposure” section
Carborne Hazard Analysis

ATC Carborne

- Speed Sensors
- Braking System
- Pick-up Coil / TWC

ATC Wayside

Speed Commands / Train to Wayside Communications (TWC)
Findings

- Ansaldo/Breda and Alstom design mitigated the identified hazards for FMEA performed at the time of manufacture.
- FMEA gaps identified between modern standards and the time of manufacture.

Remedial Actions

- FMEA gaps relegated to acceptable hazard level by equipment service history analysis.
- No modifications to onboard equipment required.
Carbourne Hazard Analysis

Mitigations using service history based safety case

- Review reported failures at all deployments
- Years/miles of operation
- Environmental qualifications

1980’s Failure Modes List

Mitigated or Tolerable Hazards

Current Failure Modes List

Potential Unknown Hazards
(failure modes not analyzed)
Wayside ATC system was reviewed to be confined to specific portions of the ATC sub-system.

Items analyzed include: GRS Generation II Track Circuit, Alstom Gen III Track Circuit, Ansaldo AF-800 & AF800W Track Circuit.
Wayside Hazard Analysis - Findings and Remedial Actions

Findings

- Generation II and III track circuit FMEA gaps identified based on standards at time of manufacture.
- FMEA's for AF-800/800W track circuits reviewed. No action required.

Remedial Actions

- WMATA is replacing all Generation II Track Circuits.
- Gen III Track Circuits revised to update power amplifier circuit.
Wayside Hazard Analysis

Mitigations

- FMEA updated to current standard for Ansaldo AF800/AF800W
- Alstom Generation III upgraded to Generation IV (safety case complete)
- GRS Generation II replacement
- Continued process improvements
  - Additional testing
  - Ferrite chokes
  - Track Circuit Monitor Tool

1980’s Failure Modes List

Mitigated or Tolerable Hazards

Current Failure Modes List

Potential Unknown Hazards
(failure modes not analyzed)
Hazard Log

Record and track hazards identified for the ATC system throughout the life of the safety analysis program
Hazard risk and mitigation strategy identified

SIGAR

Current gaps in the safety functions identified
Conclusions

- A detailed and well documented safety process to perform complete system level safety activities was followed.

- Process uses current modern safety engineering and industry standards.

- Process provides traceability which was confirmed during the process review.
Conclusions

• The analysis did not identify any hazards requiring an immediate removal of equipment from service

• Residual risk of potential hazards is reduced by implementation of recommendations either in progress or completed by Metro
Next Steps

• The final application safety case report will be provided to the National Transportation Safety Board (NTSB) for review and closure

• Identified hazards will be tracked and closed in the Hazard Log and System Implementation Gap Analysis Report (SIGAR) under the control of Metro and included within the Safety Measurement System

• Progress continues on programs for systems upgrades and replacements as well as update to process related findings