National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

August 2011 *Volume 5 Issue 8*

Loss of Detection

At the beginning of the evening rush hour on June 22, 2009, the Washington Metropolitan Area Transit Authority (WMATA) experienced the most devastating accident in its 30 year history. That day, the lead car of train 112 collided with the end car of stopped train 214 between the Fort Totten and Takoma "Metro" railroad stations (Figure 1). The operator of train 112 and eight passengers lost their lives in the accident, and at least fifty more suffered injuries related to the crash. Damaged train equipment was estimated to cost $12 million.

Figure 1: Train 112 was travelling at more than 40 mph when it crashed into stopped train 214.

Background

Automatic Train Detection

The DC Metro rail system uses a system of track circuits to determine which areas of track are occupied by passenger trains and which areas are vacant. Track circuits (or blocks) vary in length from 39 feet to 1565 feet, and devices called impedance bonds are situated between every circuit in the rail system (Figure 2). Each impedance bond acts as a receiver for one track circuit and a transmitter for an adjacent track circuit (Figure 3). An energized track circuit indicates the track circuit is unoccupied. When a train passes over a track circuit, its wheels create an alternate path for the electrical signal, preventing it from reaching the receiver bond. This causes the signal received by the module in the control room to drop below the set value, de-energizing the track circuit and indicating that the track is occupied.

Speed Commands and Loss of Detection

The Automatic Train Control System (ATC) allows the track circuits to transmit speed commands that command train speeds to maintain safe separation. The track circuits only issue speed commands to a train on a block of track indicating it is "occupied." Therefore, if a track circuit loses detection of a train, the track circuit will not transmit any speed commands to the train, and the train will default to an authorized speed of 0 mph. A following train would continue receiving speed commands from the properly operating track circuits it traverses. WMATA train operators were expected to operate trains in an automatic mode under ATC control but allowed to switch to manual control if a safety issue was perceived.

Previous Track Circuit Failure

During a rush hour backup in 2005, WMATA experienced two near-collisions between the Rosslyn and Foggy Bottom stations. In both instances, the operator of the oncoming train observed the stopped train in time to override automatic controls and apply the brakes. Each operator attributed the near-miss to a problem with speed commands and reported the incident as such to the Metrorail Operations Control Center (OCC).

Later, ATC engineers discovered that the Rosslyn near-collisions had actually occurred because track circuit C2-111 had stopped detecting trains. Results of an investigation showed WMATA that its track circuit testing procedure – which involved placing a device called a shunt at both ends of the block to simulate a set of train wheels – was insufficient. A track circuit could fail to detect a shunt (and therefore also a train) placed over the middle of the block. This discovery led WMATA to issue a safety bulletin that amended the track circuit

Malfunctioning Train Control System in Washington D.C. Causes Deadly Crash

Proximate Causes:

- **Track circuit modules fail to detect the presence of a stopped train**
- **Automated train control system transmits speed commands to the next train until the point of impact**

Underlying Issues:

- **Inadequate track module maintenance plan**
- **Failure to properly implement new procedures**
- **Absence of effective safety culture**

testing procedure: Maintenance personnel could now test circuits by placing the shunt not only at the ends of the block, but also in the middle of the block. This modified shunt placement test would allow the crews to identify malfunctioning track circuits. A software tool was developed after the 2005 near-collision to identify "loss-of-shunt" conditions and regular testing was recommended by the WMATA developers; but after the 2009 accident, no record of tests were found and no one could verify if the software tool was being used at all. Yet a WMATA engineering bulletin about loss-of-shunt had been issued in 2005. No record of receipt or knowledge of the bulletin by maintenance supervisors or crews could be found after the 2009 collision.

Impedance Bond Replacement

On June 17, 2009, a WMATA crew replaced the impedance bonds on track circuit B2-304, located between the Fort Totten and Takoma metrorail stations. This replacement was part of an upgrade program initiated in 2006. The original impedance bonds and transmitter/receiver modules had been manufactured by General Railway Signaling Company (GRS, now Alstom Signaling, Inc.), but WMATA intended to replace the impedance bonds with Union Switch & Signal (US&S, now Ansaldo STS USA) equipment. WMATA would retain the original GRS modules.

Since the impedance bonds and track circuit modules were manufactured by different companies, engineering crews needed to adjust transmitter power settings to compensate for differing resistances between the old and new impedance bonds. The crew leader stated that while the team made these adjustments, she noticed a phenomenon known as "bobbing," in which the track circuit display transitioned from 'vacant' to 'occupied' and back even though no trains were present. After leaving the site, the crew leader opened a work order to address the bobbing issue, but investigators would discover no action was taken regarding the work order from the time it was opened until the day of the accident (5 days later). The ATC maintenance technicians performing periodic testing after the new impedance bond was installed were unaware of the open work order and did not report the bobbing because it cleared by itself. The maintenance crew thought the ATC installation crew would return to continue working.

Figure 2: Each impedance bond acts as a transmitter for one track circuit and a receiver for the adjacent track circuit.

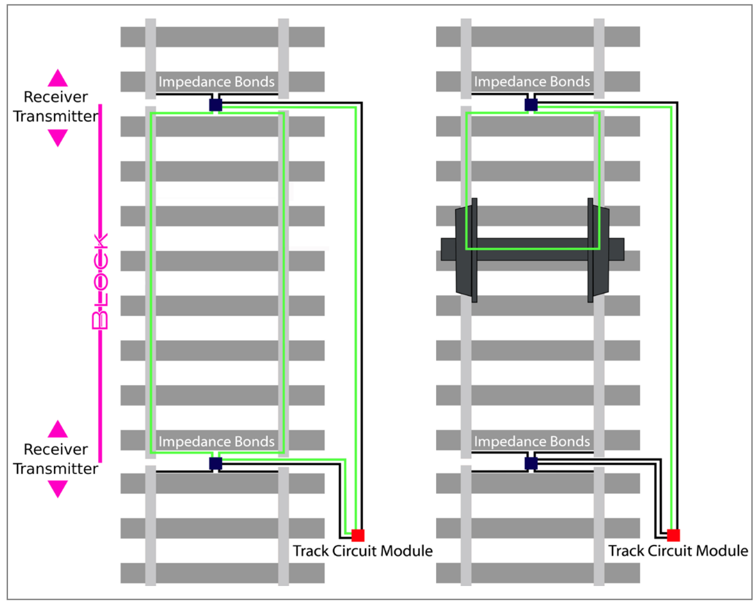

Figure 3: Diagram of unoccupied (left) and occupied (right) track circuits. The green line indicates the signal path. Track circuit modules (indicated in red) are located in a control room at the nearest train station. An energized track circuit indicates a vacant block. A de-energized track circuit indicates the presence of a train.

What Happened

At approximately 5:00 pm on June 22, 2009, WMATA Metrorail train 214 was slowly traveling on the Red Line inbound to Fort Totten station when it entered track circuit B2-304. That track circuit failed to detect the train's presence and therefore did not transmit any speed commands. As a result, train 214 defaulted to a speed of 0 mph and stopped completely within the bounds of track circuit B2-304. Train 214's operator later stated that such stops occurred often because of heavy train traffic, and he did not consider the train's behavior to be unusual. He had the train under manual control, in violation of WMATA policy at the time, but in automatic mode, the train would have braked to a stop anyway under a 0 mph speed default condition. Train 214 was not only stopped, it was now undetectable by the ATC.

Meanwhile, Metrorail train 112, which was following train 214, was receiving 55 mph speed commands. If track circuit B2-304 had been working properly, train 112 would have received speed commands to slow or stop due to the presence of train 214. Since the system read the track circuit as vacant, it allowed train 112 to travel at the maximum allowable speed of 55 mph. Sight distance tests by National Transportation Safety Board (NTSB) investigators after the crash showed that only 450 feet would have separated the two trains by the time train 112's operator saw train 214 stopped on the tracks ahead. Even though evidence proved that train 112's operator activated the emergency brakes, there was not enough distance to stop before impact. Train 112 barreled into train 214 at significant speed. Upon impact, the end car of train 214 telescoped into the lead car of train 112, eliminating passenger survival space inside train 112 for a distance of 63 feet (Figure 1). Nine people aboard train 112, including the train operator, died in the crash. Dozens of passengers were injured; emergency responders reported transporting more than fifty people to local hospitals. The damage to train equipment was estimated to cost $12 million.

Figure 4: Equipment racks inside the train control center housed track circuit modules which transmit to and receive audio frequency signals from impedance bonds in the track circuits.

Proximate Cause

The NTSB determined that the accident occurred because track circuit module B2-304 failed to detect the presence of train 214, resulting in the transmission of speed commands to train 112 until the point of impact. The module failed to detect the train because of a phenomenon called parasitic oscillation, in which a track circuit transmitter module emitted a spurious signal that mimicked a valid track circuit signal. This oscillation travelled from the module transmitter to the module receiver through the equipment racks on which the modules were mounted (Figure 4). When the spurious signal arrived at the receiver module, it produced a decaying pulse that eventually became synchronized with the track circuit frequency. NTSB determined that when maintenance crews replaced the impedance bond for track circuit B2-304, they calibrated an increase in the power of the output transistors, and this adjustment increased the amplitude of the spurious signal, giving it sufficient strength to drive the receiver module. This energized the track circuit and caused it to read as vacant.

Records showed that ever since the impedance bond was replaced, track circuit B2-304 failed to detect every train that had passed over it for five consecutive days before the accident. Investigators determined that although track circuit B2-304 did not detect the trains and therefore did not transmit any speed commands, each train's momentum carried it to the properly functioning adjacent track circuit, whose speed commands prevented the trains from coasting to a complete stop. When train 214 entered the track circuit on June 22 under manual control, it was slow enough to lack necessary momentum to carry it to the next circuit. The train stopped completely within the bounds of circuit B2-304 where it obstructed the path of train 112, setting the stage for the collision.

Underlying Issues

Inadequate Module Maintenance Plan

Before the accident, WMATA followed a GRS-recommended maintenance plan for upkeep of the track circuit modules. This involved executing a series of tests and measurements that ensured the transmitter and receiver modules operated at reasonable power and sensitivity levels. But the tests could not detect the presence of parasitic oscillation (an unknown failure mode in the system's design stage). When WMATA engineers discovered parasitic oscillation in 2005—parasitic oscillations were unknown before the Rosslyn near-miss event—they proposed a procedure to GRS, the manufacturer, to find and correct the hazard. In August 2009, as a result of the NTSB investigation, WMATA asked the manufacturer for comments on their proposed procedures. WMATA never received a GRS response other than the proposal was under study. WMATA was unwilling to implement a new maintenance practice without the manufacturer's concurrence. NTSB concluded that the modules did not function safely because the GRS maintenance plan in use could not detect or correct parasitic oscillation.

Failure to Implement Procedures

Four years before the Fort Totten accident, WMATA engineers became aware that current testing procedures could fail to identify malfunctioning track circuits, so they issued a bulletin detailing a process change—not to hunt down parasitic oscillation, but simply locate track sections that failed to detect trains. After the Fort Totten collision, NTSB interviewed WMATA technicians about their knowledge of the modified shunt-placement test developed after the Rosslyn near-collisions in 2005. None of the technicians were aware that the engineering bulletin existed. NTSB cited this fact as an indication that WMATA failed to ensure that its technicians received, understood, and acted upon critical safety information. NTSB further concluded that if the inspection procedures had been implemented and adhered to, technicians would have discovered the malfunction in track circuit B2-304 before the accident took place.

Absence of Effective Safety Culture

When NTSB reviewed WMATA's safety program, it found significant emphasis on events such as station and escalator injuries and very little emphasis on passenger safety during transit. NTSB's analysis of WMATA's safety initiatives concluded that the language, oversight, and enforcement methods pointed to a safety model that placed the responsibility for preventing accidents on its employees. Although this approach is applicable to some risks (such as those faced by trackside workers), it excludes situations such as the Fort Totten accident, which the NTSB considers to be an "organizational accident" that could not have been predicted or prevented by individual workers. NTSB went on to criticize WMATA for having "an anemic safety culture," evidenced in part by its failure to address audit findings and its backlog of open work orders. In the words of a maintenance supervisor, 'the mentality was to run trains.'

NTSB describes organizations with effective safety cultures as ones in which "senior management demonstrates a commitment to safety and a concern for hazards that are shared by employees at all levels within the organization." Contrary to this definition, NTSB found deficiencies in the way WMATA approached safety concerns, including propagating a climate that placed schedule over safety throughout the organization. For example, work orders that affected railway congestion were given priority over other issues - such as track circuit malfunctions – that could adversely impact passenger safety during transit. Scheduled maintenance actions to head off track circuit problems proved ineffective, evidenced by the track circuit B2-304 work order of June 18, 2009 to test a newly installed impedance bond. Technicians identified a problem with the track circuit's function, but no action was taken regarding the work order from the time it was opened until the day of the accident because they assumed the installation crew would return to address the problem.

WMATA ineffectively distributed safety-critical information throughout the organization and then failed to assess whether or not the new protocols were being followed. This trend could be traced as far back as 1996, when the NTSB observed that WMATA employees “reported a perceived lack of communication and a sense of information isolation within the organization.” Unfortunately, as evidenced by technician interviews from the TSSM (track, structures, and systems maintenance) department, NTSB concluded that WMATA’s poor internal communication prevented it from adequately applying lessons learned from past failures to prevent future accidents. WMATA’s approach to these concerns displayed a distinct lack of hazard recognition, risk assessment, and corrective action implementation. As per NTSB, the sum of these shortcomings indicated the presence of severe flaws in the Metrorail safety culture before the Fort Totten collision.

Aftermath

In its official report, issued October 2010, NTSB made several recommendations to WMATA and its oversight committee. The board recommended that WMATA review and revise its process for disseminating technical bulletins and other safety-critical information. NTSB emphasized WMATA’s responsibility not only for disseminating the information, but also for ensuring that its employees understand and take appropriate steps to apply the information. The board also directed WMATA to work with GRS/Alstom to develop a periodic module inspection procedure that would allow technicians to identify parasitic oscillations, such as the one that caused track circuit B2-304 to lose detection. NTSB issued an identical recommendation to several other transportation authorities around the country which are known to use circuit modules identical to the one involved in the Fort Totten accident. In August 2010, the general manager of WMATA published a column in the *Washington Post* promising that all NTSB recommendations would be implemented.

For Future NASA Missions

According to Dr. James Reason, Professor Emeritus at the University of Manchester and author of *Managing the Risks of Organizational Accidents*, organizations with effective safety cultures exhibit characteristics of informed cultures, learning cultures, just cultures, and reporting cultures. That is, effective safety cultures continually collect, analyze, and disseminate safety critical information; adapt based on lessons from the past; and encourage employees to report safety-related information while fostering both individual and organizational accountability. Per NTSB, WMATA exhibited deficiencies in all of these areas, but the Fort Totten accident was most directly impacted by WMATA’s failure to adapt after identifying the circuit malfunction that caused the Rosslyn near-collisions. This points to flaws specifically in information and learning culture aspects.

Although cultivating an informed safety culture at NASA requires action on multiple fronts – not just on information sharing and learning – NASA can use this incident as a reminder of how mission success rests partly on the degree to which management ensures that lessons from failures are published and integrated into planning and operations. Such information is useless unless it stimulates productive change. We can prove we’ve learned from failure when we can trace the rationale for how we work to such learning. Dr. Reason wrote in *Managing the Risks of Organizational Accidents*, “the two characteristics most likely to distinguish safe organizations from less safe ones are, firstly, top-level commitment and, secondly, the possession of an adequate safety information system.”

Questions for Discussion

- **Have you assessed the safety culture surrounding your project recently?**
- **What criteria did you use to gauge your project’s safety culture?**
- **Have you identified ways to improve communication, reporting, or information sharing related to your project?**

References

Johnson, Matt. “Metro Track Circuit Example” Online Image. 25 Feb 2010. < http://www.flickr.com/photos/39017545@N02/4387502330/>.

Morrissey, Aaron. “NTSB Hammering WMATA at Red Line Crash Hearing.” DCist. 27 July 2010. < http://dcist.com/2010/07/ntsb_hammering_wmata_at_red_line_cr.php>.

National Transportation Safety Board. Railroad Accident Report: Collision of Two Washington Metropolitan Area Transit Authority Metrorail Trains Near Fort Totten Station. Washington D.C., October 2010.

Sarles, Richard. “Changing the safety culture at Metro.” The Washington Post. 15, Aug 2010. < http://www.washingtonpost.com/wp-dyn/content/article/2010/08/13/AR2010081305793.html>

Sumwalt, Robert. “Roadmap to Safety Culture.” National Transportation Safety Board, September 2010. < http://www.ntsb.gov/speeches/sumwalt/Transit-Rail-Advisory-Committee.pdf>.

Zhang, Hui et al. “Safety Culture: A Concept in Chaos?” Proceedings of the 46th Annual Meeting of the Human Factors and Ergonomics Society, 2002.

SYSTEM FAILURE CASE STUDIES

NSC

NASA SAFETY CENTER

Responsible NASA Official: Steve Lilley steve.k.lilley@nasa.gov

Developed by: ARES Corporation

Thanks to the National Transportation Safety Board for its invaluable peer review.