

Diabolical Deeds in the District

District of Columbia Metropolitan Area Transit Authority (Team 1)

Final Agency Report

1 March 2017

Anthony Bertone | George Cornick | Allen Fidler | Conor Pierce | Naim Ziab

Contents

[Orientation 3](#_Toc481430158)

[Mission Statement 3](#_Toc481430159)

[Organizational Information 3](#_Toc481430160)

[Bottom Line Up Front 4](#_Toc481430161)

[Problem Statement 4](#_Toc481430162)

[Purpose 4](#_Toc481430163)

[Scope 4](#_Toc481430164)

[Constraints 4](#_Toc481430165)

[Elements of the Investigation 5](#_Toc481430166)

[Operational Space 5](#_Toc481430167)

[Objects/Subjects of Investigation and Roles Played 5](#_Toc481430168)

[Analytic/Investigative Methods 5](#_Toc481430169)

[Findings 6](#_Toc481430170)

[General Finding Statement 6](#_Toc481430171)

[Specific Findings 6](#_Toc481430172)

[Secure Area/System Access 6](#_Toc481430173)

[Property Inspection 7](#_Toc481430174)

[Employee Supervision 8](#_Toc481430175)

[Employee Quality Assurance 9](#_Toc481430176)

[Open Issues 9](#_Toc481430177)

[Analysis 10](#_Toc481430178)

[Appendix 10](#_Toc481430179)

[I. Evidence Inventory 10](#_Toc481430180)

[II. Association Chart 15](#_Toc481430181)

[III. Sequence of Events Overview 16](#_Toc481430182)

[IV. Main ACH Hypotheses - What Happened? Were policies infringed? 17](#_Toc481430183)

[A. Main-sub ACH Hypothesis - What Happened? Accident or Sabotage? 17](#_Toc481430184)

[V. Unauthorized Access ACH Hypotheses 17](#_Toc481430185)

[VI. Bag Check ACH Hypotheses 17](#_Toc481430186)

[VII. Employee Quality Assurance ACH Hypotheses 18](#_Toc481430187)

[A. Jones Toxicology ACH Hypotheses 18](#_Toc481430188)

[B. Douriri Involvement ACH Hypotheses 18](#_Toc481430189)

[C. Mr. Smith/Social Group Involvement ACH Hypotheses 18](#_Toc481430190)

[VIII. Inadequate Supervision ACH Hypotheses 18](#_Toc481430191)

# Orientation

1 April 2011 saw thousands of visitors traveling to Washington, D.C. for the annual Cherry Blossom festival. At 10:55am a Blue line train collided with a packed, Orange line train, carrying the Japanese Prime Minister, at Farragut West Station. The collision resulted in 34 deaths and over 200 injuries.

# Mission Statement

The D.C. Metropolitan Area Transit Authority’s (MTA) mission is to *operate and maintain a safe, reliable and effective transit system that enhances mobility, improves the quality of life, and stimulates economic development in the Washington metropolitan area*.

The MTA internal review team was tasked with determining the cause of the collision and determining what future action(s) should be taken to prevent a similar tragedy from occurring in the future.

# Organizational Information

Team Leader - Naim Ziab. Ziab was responsible for ensuring all team members had the proper tools to complete their job, as well as facilitating communication among team members. Ziab was ultimately responsible for ensuring all deadlines and deliverables were met.

Association Analyst - Allen Fidler. Fidler was responsible for creating and updating an association chart containing all individuals and significant events within the scope of the MTA internal review.

Event Sequence Analyst - Anthony Bertone. Bertone responsible for creating and updating a sequence of events chart for all significant events within the scope of the MTA internal review.

Evidence/Hypothesis Analyst - Conor Pierce. Pierce was responsible for maintaining an evidence inventory containing all relevant pieces of information from the review for use by the other analyst. Pierce also utilized specialized software in combination with the evidence inventory to develop and rate hypotheses regarding the review focus.

Editor/Presenter - George Cornick. Cornick was responsible for assisting all other team members in their analysis, as was well as turning communicating the MTA’s position in oral and written forms.

# Bottom Line Up Front

Improper and insufficient policy enforcement and management within the MTA led to the compromise of the rail system, which ultimately caused the 1 April train collision. The collision resulted in a massive number of injuries and loss of life, and damage to the United States national security, as well as damage to the MTA reputation with riders and potential riders. Without serious policy revision, similar or worse instances are possible.

# Problem Statement

## Purpose

The investigative focus of the D.C. MTA was to determine if a lack of policies and/or failure of existing policies were the culprit of the train collision. If determined to be at fault, the investigative focus also included the recommendation of policy creation or revision to prevent similar events from occurring again.

## Scope

The D.C. MTA’s range of focus was a complete policy review in the areas of administration, maintenance, operations and security.

## Constraints

The MTA was faced with various constraints in relation to the Metro system and legal authority. As the MTA organization, it is our duty to implement policies that we believe will protect our loyal commuters. That said, there is no way for us to predict sabotages to our system, such as the 1 April collision. Our best effort to eliminate instances as such solely relies on our ability to implement policies that will deter against acts of sabotage.

Another constraint the resides with the MTA is our knowledge on the collision mishaps and safety system controls. It is beyond our scope of expertise in the technical aspect as to how the automatic braking system was disarmed. We can only implement policies which eliminate access to these control rooms. It is the responsibility of manufactures and the NTSB to make sure safety systems are tamper proof.

A legal constraint for the MTA is our legal authority. With no right to prosecute or detain, policies to only discourage criminal behavior can be leveraged. In criminal cases we must rely on police and FBI for further investigations.

# Elements of the Investigation

## Operational Space

The MTA’s internal review centered around the scene of the collision at Farragut West Station, 900 18th St. NW Washington, DC 20006, and expanded outward from there. Other key locations involved in the investigation are: McPherson Square Station, 1400 I St. NW Washington, DC 20005, the section of track in between Farragut West and McPherson Square stations, the MTA Pass & ID office, and the MTA maintenance yard.

## Objects/Subjects of Investigation and Roles Played

* Blue Line train - Blue 17, sabotaged train involved in collision
* Orange Line train - stationary train involved in collision
* Hydrogen Cyanide backpacks - WMD near collision scene
* Mohar Abul-Nassar - MTA employee
* Rahim Douriri - MTA employee
* Douglas Fredericks - MTA employee
* Quentin Jones - blue line train conductor
* Dontel Smith - MTA shift supervisor

# Analytic/Investigative Methods

The MTA internal review team utilized the analytic methods taught in the SRA 231 class at Penn State University. The team specifically worked under the Information-Sense Making-Communication analytic workflow. The team sorted through the data presented to collect pieces of evidence and inventoried this using an Excel workbook (see Appendix I). The team then moved onto Sense-Making by using the collected evidence in conjunctions with analysis tools. The team used to Analyst Notebook to create an association chart, as well as a sequence of events (see Appendix II and III ). From the evidence inventory and Analyst Notebook products, the team developed hypotheses as to how and how much the MTA was responsible for the 1 April collision. Utilizing Analysis of Competing Hypotheses software, the team rated evidence and determined the least inconsistent hypotheses (see Appendix IV).

General description of analytic approach

# Findings

## General Finding Statement

The MTA has concluded the cause of the train collision on 1 April was due to an act of sabotage due to MTA lax policies. The Metro system was vulnerable to insider threats which allowed this act of sabotage to occur. This finding was determined after examining four aspects: secure area/system access, property inspection, employee supervision, and employee quality assurance. Our security system was infiltrated with the help of metro employees, which needs to be prioritized. Unauthorized and abused access was identified in sensitive areas of the metro station. Our ability to maintain employees engaged in unsupervised and unauthorized activities in events leading up to the 1 April collision was not adequate. Poor employee quality assurance has been identified through malicious actors and their connections with metro employees.

The MTA internal review revealed four major points of failure that allowed the Metro system to be taken advantage of: secure area/system access, property inspection, employee supervision, and employee quality assurance.

## Specific Findings

### Secure Area/System Access

After analyzing the Sequence of Events chart, the internal review team became concerned with a number of instances involving unauthorized access to what should have been secure areas and systems in a short period of time prior to the collision. The three main areas of concern are: Pass & ID operations, employee locker room, and track area.

MTA employee Rahim Douriri was hired as a Pass & ID employee; however, after performance issues, was moved to completing miscellaneous odd jobs by former MTA shift supervisor Dontel Smith. Douriri stayed on the payroll system as a Pass & ID employee. On several occasions, Douriri accessed the Pass & ID office outside of normal business hours, including the morning of the collision at 5:00am. Douriri was a no-show for his shift that had a later start time on 1 April. Douriri’s ID was found in an ambulance on 1 April stating he was a yard maintenance employee. This does not match with his payroll file as a Pass & ID employee. Within the month prior to the collision, Douriri was involved in an incident involving 5 ID cards being unaccounted for. From this information, the team assumes the unusual actions of Douriri are linked to the compromise of the rail system.

Former MTA employee Douglas Fredericks’ ID was recovered after the 1 April train collision with some irregularities. The ID had an issue date of 2 February 2004. The issue date is entered manually by the employee creating the ID. The ID had a creation date of 8 March 2011 at 2:00am (outside Pass & ID business hours). The creation date is automatically embossed on the back of the ID by the printing machine. Of more concern regarding this ID is the fact that Fredericks was let go by former MTA shift supervisor Dontel Smith on 6 March 2011. An MTA vehicle was involved in a motor vehicle collision on 1 April. The driver provided Metro Police with a Douglas Fredericks ID. The MTA assumes this forgery is connected with the 1 April malicious events.

Quentin Jones, the blue line train conductor involved in the collision, was determined to be deceased prior to impact via his blood toxicology. Jones had to history of drug abuse. Jones was only known to be taking pain medicine, i.e. Motrin, for previous knee injuries, that was kept in his employee locker. Jones died from a codeine overdose, thus preventing him from manually stopping the blue line train. The MTA has no specific evidence pointing to the intentional compromise of Jones’ pain medicine to induce the overdose; however, the MTA assumes this was potentially a point of attack for malicious actor(s).

On 28 March 2011, security camera replacement was completed in the track area just prior to the scene of the collision. Between this date and 1 April, unknown actor(s) were able to gain access to this area and paint over the cameras to cloud their visual. There is no specific mechanical or electrical system in this area that can be compromised to allow a collision between two trains to occur. The MTA assumes this vandalism was done to mask the movements of malicious actor(s).

From this evidence, the MTA infers malicious actor(s) were able to easily gain access to what should be secure areas/systems, potentially through inside help, to sabotage rail operations for a collision to occur.

To mitigate these security breaches, the MTA is recommended to implement a new ID authorization system with a few specific enhancements. First, when a new ID is created, the receiving party must be in the payroll system and the privileges assigned to the receiver must match their work area as defined in the payroll system. Second, sensitive areas, such as the Pass & ID officer, are not accessible after business hours.

### Property Inspection

On 15 March 2011 transit police were suspended from randomly stopping passengers when entering stations to examine their property for traces of explosives after a rider Advisory Council meeting due to privacy concerns.

On 4 April 2011 two backpacks containing Hydrogen Cyanide were discovered along track two, which is in the area of the 1 April train collision. It is theorized that the weapon was intended to be used as part of a terrorist attack.

The presence of the backpacks in and of itself do not explain why or how the trains collided. What it does do is show a large security weakness for the MTA. The team has no reason but to assume that if a chemical weapon was so easily able to be not only brought into our track area, but go undetected for some time, this lax security policy may have been taken advantage of by malicious individual(s) who brought in equipment with the same ease to cause the train collision.

The MTA infers malicious actor(s) took advantage of the security weakness to move about and transport equipment undetected.

To resolve this issue for the future, the MTA is recommended to implement 24 hour/7 days a week property inspection for random passengers at each station. The MTA police department is also recommended to conduct short sweeps of random sections of track each day.

### Employee Supervision

The MTA reviewed two specific instances of inadequate supervision related to the 1 April train collision matter.

MTA safety inspectors discovered unauthorized work being done in the track area within the month prior to the train collision by four MTA employees. This activity occurred between McPherson Square and Farragut West stations, in the area of the vandalized security cameras from the Secure Area/System Access section above. It is unknown exactly what was done, but it involved the MTA vents 22 and 24. Vent 22 terminates in a privately-owned courtyard at street level. The MTA assumes the vents were used for the discrete travel of malicious actor(s).

Blue 17, the blue line train involved in the 1 April collision, was running an eight-car train at the time, rather than its normal four or six cars. After investigation of the sequence of events that permitted the additional cars, the team revealed only half of the authorized signatures were obtained. MTA engineers assure the additional cars did not contribute to the excessive speed and ultimate collision. The engineers are confident the additional brake wheels would assist in slowing the train down. The MTA assumes that minimal authorization enforcement in this case and others contributed to the ease of compromise of rail operations on 1 April.

The MTA infers that the inadequate supervision policy and enforcement in events leading up to the 1 April collision allowed malicious actor(s) to forward their movement in disguise of official MTA business.

The MTA is recommended to implement a work authorization and signature tracking system to minimize the discrepancies that allowed unauthorized or authorization in process activity to occur.

### Employee Quality Assurance

In review of the association chart, the MTA has determined it was irresponsible in employee quality assurance. The association chart revealed links between MTA employees and known malicious actor(s).

After investigating Rahim Douriri’s 1 April no-show shift, the internal review team discovered Douriri boarded a flight out of the country. Further investigation revealed this was one of several flights outside of the country in the recent months. Douriri is primarily a student in the United States. Dr. Ahmed ibn Yussuf, a visiting Egyptian professor, is Douriri’s PHD supervisor. Douriri shared an apartment with former MTA employee and fellow student Mohar Abul-Nassar. Abul-Nassar’s whereabouts are currently being seeked by the Egyptian National Police. Abul-Nassar was found deceased from cyanide poisoning upon Douriri’s return from his most recent flight. The MTA assumes Douriri’s suspicious activity regarding Pass & ID operations, his frequent travel out of the country, and deceased roommate are linked to the suspicious conditions of the 1 April collision.

Former MTA shift supervisor Dontel Smith was wanted for questioning in connection with the 1 April Sumter-Dodge jewelry heist by D.C. Metro Police. Smith was found shot to death prior to questioning. D.C Metro Police report former MTA employee Douglas Fredericks is responsible for the death of Smith; however, Fredericks died of cyanide poisoning while in police custody. The MTA assumes both deaths are related to Abul-Nassar’s death, as well as several other deaths reported to occur after the 1 April events via cyanide poisoning.

The MTA infers corrupt MTA employees and former MTA employees allowed rail operations to be compromised on 1 April and ultimately the train collision.

The MTA is recommended to implement continuous background investigations and their associated testing (e.g. drug testing) throughout an employee's career. This will ensure employees are continually meeting company standards by allowing the MTA to request criminal and other records.

## Open Issues

As the MTA is not a criminal investigation agency, the motive, intent and person or persons responsible for sabotaging the Metro system and the 1 April collision needs to be determined by the FBI and D.C. Metro Police.

The MTA is not tasked with providing collision reconstruction or determining the mechanical systems at fault or that were disrupted that allowed the collision to occur. This is the responsibility of the National Transportation Safety Board (NTSB).

# Analysis

In the first week or two of investigation the teams’ hypotheses and associated Analysis of Competing Hypotheses (ACH) tables mainly focused on how the crash occurred. This included hypotheses on physical aspects like the failure of the braking system, who was involved, and things of that nature. Although this wasn’t our main focus as the MTA, the team wanted to get an understanding of what happened before recommending policy changes or new policy implementation. After a good understanding of what happened was obtained, the additional information received in the third week of the investigation led the team to realize the seriousness of the MTA’s lax policies. The ACHs morphed to pertain to more policy specific topics (i.e. hypotheses on what policies were not followed) which gave the team a good understanding of what policy revisions were needed.

As mentioned above our association chart played a key role in visual showing the connections our employees had. The association chart showed us clear links between our employees and possible criminal activity. This led us to conclude that aspects of our employee quality assurance (ie background checks) needed to be strengthened.

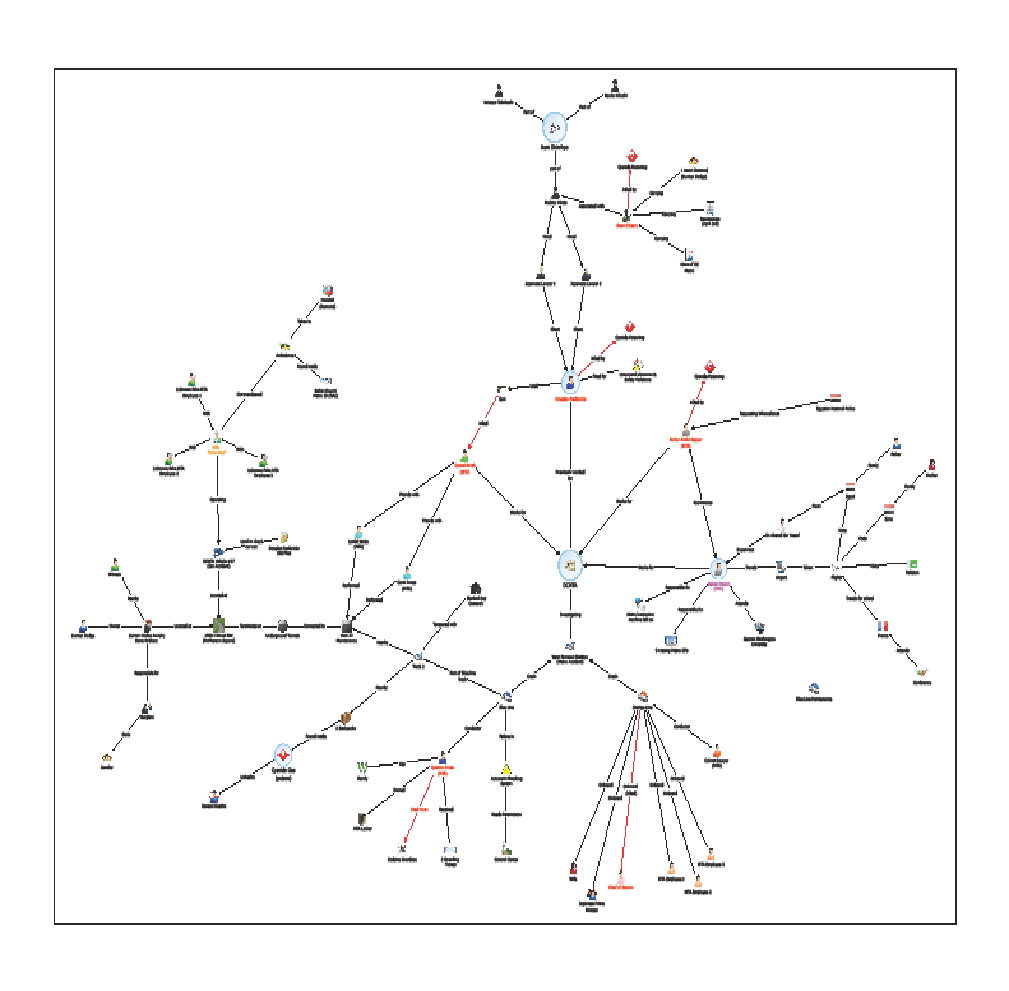
Our sequence of events timeline also played an important role showing us issues with employee quality assurance and inadequate supervision. It laid out a very understandable timeline that clearly showed multiple instances where employees weren’t doing what they were supposed to. This led us to conclude that necessary changes need to be done to these areas. Our current policies surrounding supervision is just not enough to ensure foul play isn't happening in our workplace.

# Appendix

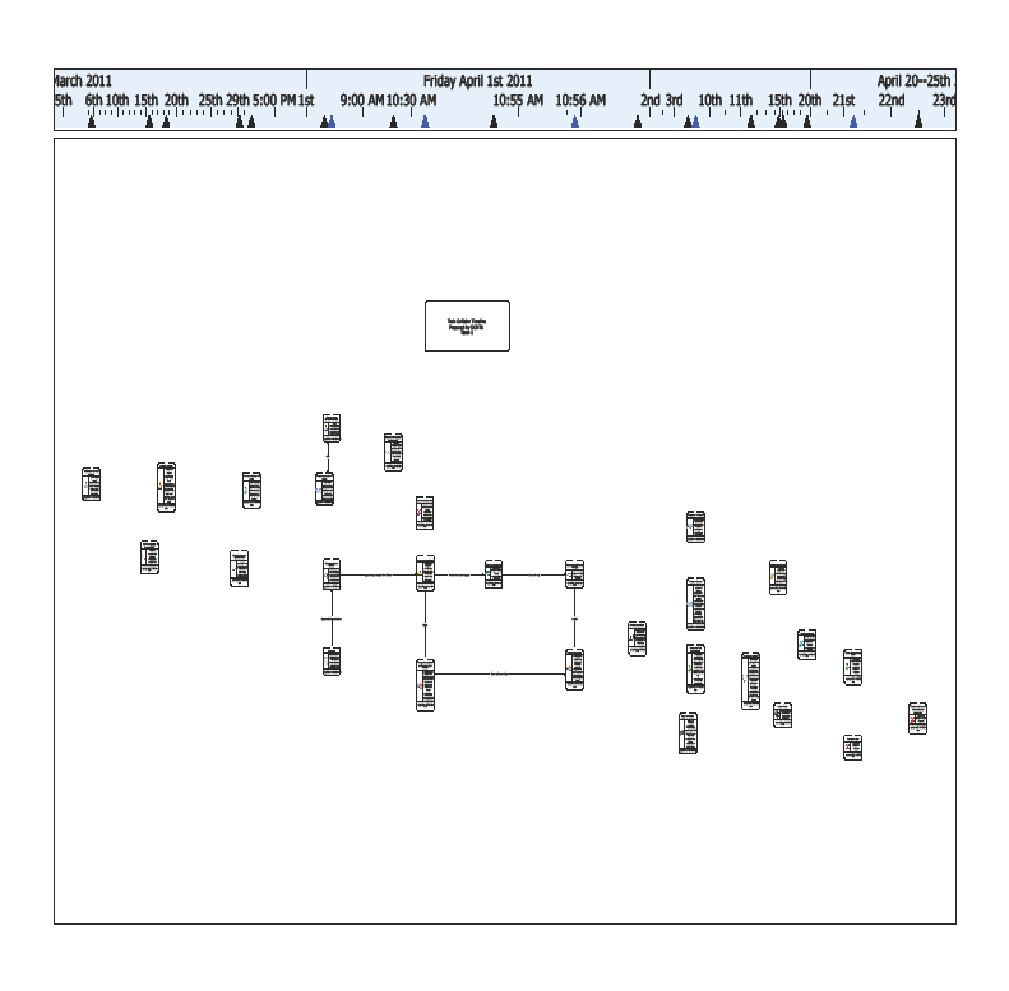
# Evidence Inventory

|  |  |  |  |
| --- | --- | --- | --- |
| **Problem:** | | | |
| **Key Analytic Question:** Why did the trains collide? | | |  |
|  | **Evidence** | **Evidence Type** | **Assumption/Inference:** |
| 1. | Blue 17 was an eight-car train instead of a six-car train | Physical | Someone messed up on the car count for the train |
| 2. | An excessive speed alert is triggered at the Farragut West Station for the Blue train | Digital | The alert system was working properly, could have been ignored |
| 3. | A warning was sent out for the Blue Line | Digital | Communication to the train was working properly |
| 4. | The Blue Line Train impacts the Orange Train at 72 MPH | Physical | The driver did not stop the train |
| 5. | The Blue Line driver was on drugs | Forensic | Driver has passed previous drug tests, could have been drugged |
| 6. | Automatic braking system failed to engage | Direct | The train needed to be checked more for issues |
| 7. | Orange Line was in station 4-5 minutes after scheduled departure | Direct | Train could have been running late that day |
| 8. | Blue Line was in for maintenance that morning | Direct | The train was not properly checked |
| 9. | Blue line driver had previous speeding tickets | Direct | Previous speeding tickets were not substantial and were a long time ago and are common for drivers, most likely not the cause |
| 10. | Jones didn't even drink and was very involved in the community | Direct | Leads us to believe that Jones was mostly drugged by someone else |
| 11. | Jones was hooked on Motrin for | Direct | Jones could have overdosed |
| 12. | Toxicology report determines Jones was indeed dead before impact | Forensic |  |
| 13. | Driver involved in vehicle mishap was no longer on MTA payroll | Direct | People are clearly posing as employees of the MTA with legitimate ID cards |
| 14. | MTA John Doe was posing as an employee using the same name (Mr. Fredericks) the driver involved in the vehicle mishap used | Direct | Outside forces are posing as Mr. Fredericks |
| 15. | ID for Douriri found in ambulance has him labeled as a yard maintenance worker when really he works in Pass and ID | Physical | People who weren’t supposed to had access to the maintenance yard which could have led to a train being sabotaged |
| 16. | ID labeled for Mr. Frederick was found and issue date February 2nd 2004 is well before creation date of March 8th 2011 | Physical | Evident that ID’s are being created and used for malicious purposes |
| 17. | Real Mr. Frederick was let go on March 6th | Direct | Mr. Frederick most likely isn’t involved, people are posing as him |
| 18. | Three metro workers helping their supervisor Mr. Smith out at the crash site do not recall pulling someone out of the crash site with MTA John Doe’s injuries | Direct | MTA John Doe and the three people that got him in the ambulance do not work for the MTA and are most likely involved in suspicious activity |
| 19. | Douriri has not been seen since March 31st and is unable to be located | Direct | Could be hiding from authorities |
| 20. | Douriri accessed the Pass and ID office at 5am on April 1st and didn’t show up to his shift that day | Physical/  Direct | Was in there when he shouldn’t have been and then didn’t show up for work that day |
| 21. | Douriri was involved in mishap back on March 5th where 5 ID cards went missing, 3 days later he left the Pass and ID door open and lamination machine on | Direct | Douriri is most likely involved in how the people posing as MTA workers got their IDs |
| 22. | Mr. Smith retasked Douriri to do miscellaneous jobs due to his lackluster efforts at worm | Direct | Douriri wasn’t focused on work |
| 23. | 2 MTA workers were hurt working on Vent Stack 22, not owned by the MTA, which opened to a court yard below | Direct | They were involved in suspicious activity, we believe this may be related to the robbery |
| 24. | Deputy Chief DC Metro Police Transit Police interview with Mr. Smith and his two maintenance workers did not happen as all 3 were a no show and are supposedly sick | Direct | The 3 no shows are not a coincidence, they are most likely hiding something |
| 25. | Abul-Nassar, roommate and shift splitter with Douriri, told the Deputy Chief DC Metro Police Transit Police that Douriri is “out of town” | Direct | Douriri could be evading law enforcement |
| 26. | Douriri made two trips to Egypt in 2008 and 2009 where he cited family reasons | Direct | Could have been for other malicious reasons |
| 27. | Douriri is currently in Marseille, France for what he cited as an academic conference | Direct |  |
| 28. | Douriri and his school supervisor Yussuf are not on DHS terror watch list | Direct | Not on the watch list so they don’t have any terroristic ties that we know of |
| 29. | Deputy Chief DC Metro Police Transit Police found the paperwork signed by Mr. Smith authorizing Blue 17 to run as 8 trains | Direct | Blue 17 was authorized internally by Mr. Smith, he did not show up for the interview which is suspicious |
| 30. | Tunnel cameras near vent stacks 21/22 have been painted over | Physical | We think this was the act of the robbers as whatever happened to the train occurred before this point |
| 31. | Backpacks containing cyanide gas were found near vent stacks 21/22, across from the painted over cameras, three days after the April 1 accident | Physical | We think the backpacks were supposed to be released into the tunnel but Douriri and his men got interrupted by the robbers |
| 32. | Backpacks also had triggers in them for detonation, bags were useless left behind | Physical | We think that these backpacks were supposed to be used but Douriri and his men got interrupted by the robbers before detonating them |
| 33. | MTA employee Dontel Smith was found shot dead outside his apartment, was being investigated for robbery, Douglas Fredericks has been arrested/has confessed | Direct | We believe that Smith and Frederick were involved in the robbery together |
| 34. | Frederick worked for Smith at the MTA, was fired awhile back, stated murder was revenge for being fired | Direct | We don’t think that Frederick killed Smith for work related reasons, as the investigators stated this seems to easy |
| 35. | Frederick collapsed during interrogation from what eventually was deemed from cyanide poisoning | Direct | Frederick along with the other MTA workers involved in the robbery/attack were also poisoned |
| 36. | Two lawyers came in as Frederick was being taken out on an ambulance claiming they were his lawyers, walked right past Frederick (claimed they know him but didn't recognize him being taken out), the Japanese lawyers are usually associated with money laundering not murder | Direct | We think that the lawyers are tied to the terrorist attack as we think that the terrorist group was of Japanese origins and they seem out of place considering they usually deal with money laundering. |
| 37. | Interpol fugitive Swan O’Leary was found dead, poisoned by cyanide, in Canadian territory of Pelee Island, found with 1-karat diamond with SD stamp, has ties to Japanese terrorist group | Direct | Was clearly involved in the robbery cause of the initials SD, was killed by same people as Frederick, another tie to Japanese terrorism |
| 38. | Abul-Nassar, roommate of Douriri was found dead in their apartment from apparent cyanide poisoning | Direct | Killed by same people as others who were poisoned |
| 39. | Douriri is back from his overseas travel, offering complete statement on the finding of his dead roommate | Direct | We still think Douriri is involved with the conspiracy because of his false ID card |
| 40. | Jones toxicology report indicated he was multiple times over the lethal dose of codeine | Forensic/Direct | Was drugged rather than willingly overdosed |
| 41. | Bag checks were recently suspended by the advisory council | Direct | Relates to the backpacks found by vent stacks 21/22 |

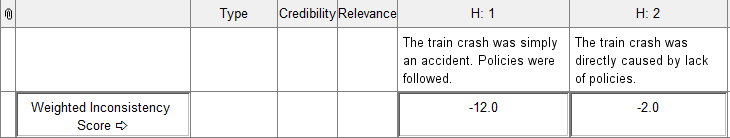
# Association Chart



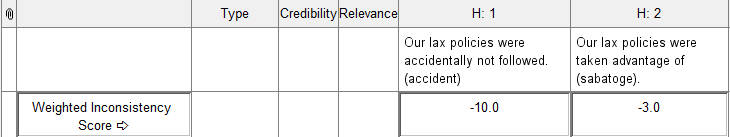
# Sequence of Events Overview



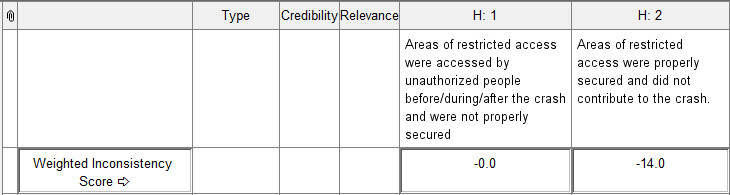
# Main ACH Hypotheses - What Happened? Were policies infringed?



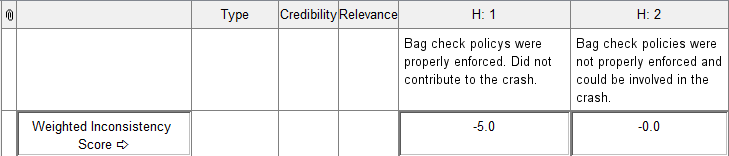
## Main-sub ACH Hypothesis - What Happened? Accident or Sabotage?



# Unauthorized Access ACH Hypotheses

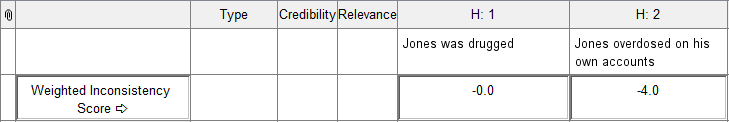


# Bag Check ACH Hypotheses

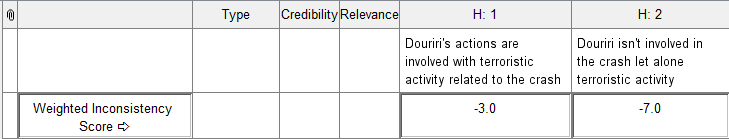


# Employee Quality Assurance ACH Hypotheses

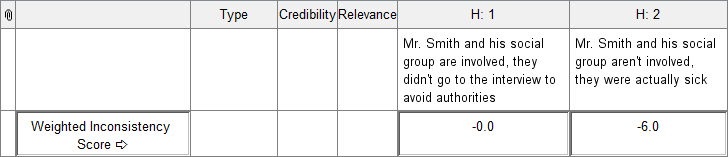
## Jones Toxicology ACH Hypotheses



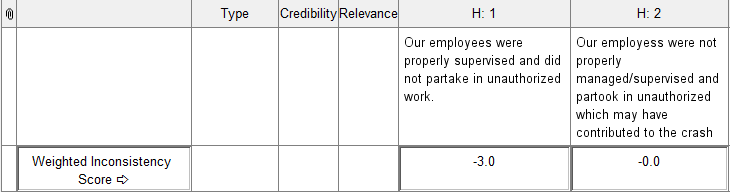
## Douriri Involvement ACH Hypotheses



## Mr. Smith/Social Group Involvement ACH Hypotheses



# Inadequate Supervision ACH Hypotheses



\*See attached documents for full ANB and ACH files