

## US Infrastructure Reliability: The Disney Monorail Catastrophe

Joseph A. Childs, PE  
Lockheed Martin Corporation  
Email: joseph.childs@ieee.org

On July 6, 2009, two monorail trains at Walt Disney World in Orlando collided, taking the life of the young conductor of one of the trains. Although many safety measures were instituted and followed, this accident still occurred. The premise of this paper is to investigate the idea whether some of the standard practices used in the reliability and safety community could have helped prevent this catastrophe, or if it was a “one-in-a-million” occurrence that could not have been avoided.

### 1. INTRODUCTION

*“It’s a bit shocking. Disney seemed so perfect”*

*– Danielle Williams (London tourist)  
on the fatal monorail crash  
at Walt Disney World, July 5, 2009*

Austin Wuennenberg was working in his “dream job” as the pilot of one of the sleek Walt Disney World Monorails. He was heading into his final stop at Disney World at the end of a long day. Meanwhile, another Disney monorail pilot was backing his monorail into a spur so it could be stowed for the night, or so he thought. However the tracks did not switch as expected, so the train continued to back down the main track where Mr. Wuennenberg’s vehicle was travelling. By the time the backing train could be seen, it was too late. Neither could stop in time, so they collided. Mr. Wuennenberg was crushed in the cockpit, trying to stop his train. His life was snuffed at approximately 2:00 AM on July 5, 2009.

But how could this happen? The monorail has been operating for years; this was the first fatal accident of the monorail system in 38 years! The Disney World monorail system was outfitted with automatic sensors, designed to prevent such crashes. What lessons can be taken from this accident?

### 2. HOW COULD THIS HAPPEN?

The Disney monorail system was designed with checks and balances to assure such a thing could not occur.

- There was the moving blocklight system (MAPO) system, designed to stop trains automatically, if they travel too close to one another. The MAPO device is installed in the top center of the pilot’s console. It has a pushbutton for “override,” and three lights: red, yellow, and green. Green indicates there are greater than 1,500 feet to the nearest train, yellow means between 1,500 and 500 feet. Red is a warning that the train is becoming unsafe, so the on-board computer locks out the pilot’s speed control capability, and brakes the train.
- Inspections and systems checks are performed daily to assure all systems, including the MAPO, is working properly.
- The MAPO system must be manually overridden to back-up into a spur for stowing. Multiple employees are required to verify track switch positions when such maneuvers must take place.
  - There is a series of sensors that monitor the positions of the locks that hold the switches, and say which section of track has power.
  - The sensors are displayed on a grid for the Switch Operator in the Maintenance Shop, as in Fig. 1. A similar display is located at the Central Coordinator’s station in the Transportation Ticket Center.
  - The Central Coordinator monitors the whole system, and communicates by radio. When a switch is moved, there was a step-by-step protocol of radio communication between the

train driver, the central coordinator, and the maintenance operator to assure all is properly positioned.

- A video camera image is also displayed at the Maintenance Shop for the Switch Operator.

However, this event indicates these precautions were not fool-proof.

- The MAPO system was installed to stop trains automatically, if they came too close.  
*This system was disabled to allow transfer of a train off the Epcot loop to place the train out of service for the night.*
- The operators are in communication via a radio network throughout the monorail system.  
*According to the Orlando Sentinel, “People familiar with the investigation say a worker mistakenly radioed that he had activated a track switch that would have allowed the train to reverse off the Epcot beam and onto a spur leading away from the main track; the train instead wound up backing down the Epcot beam and into a train piloted by Wuennenberg.” [1]*
- There were sensor and video displays, and a step-by-step procedure; the Central Coordinator was to oversee the whole operation.  
*At the time of the accident, Disney policies did not require the coordinator to be positioned at that console. Again, the Orlando Sentinel, citing personnel familiar with the investigation details, “The central coordinator’s role was also in flux that night — an employee had gone home ill, so the job was being handled temporarily by a manager on his dinner break — so no one was at the console in the Transportation and Ticket Center.” [2]*

### 3. SUMMARY OF FINDINGS

Based on its investigation that started in July, the U.S. Occupational Safety and Health Administration (OSHA) cited Disney for a “serious safety violation” that contributed to the July 5 accident. In particular, it was noted that the manufacturer of the monorail, Bombardier, Inc. (Montreal), had included in its operational guide the caution to use a spotter behind a train, when it is in reverse. This notice is printed in bold lettering under the heading, “Moving the train in reverse direction.” [2]

Disney has instituted additional measures, including the spotter requirement, in its standard practices. Even if a train overshoots a stopping point by 1 to 2 feet at a station, it must wait for a spotter to clear the maneuver via radio before backing-up to align the cars and gates.

OSHA is expected to release its report in early January, 2010. The National Transportation Safety Board is independently investigating this event, as well.

### 4. RELIABILITY ENGINEERING TOOLS – ARE THEY ENOUGH?

Like most large high-profile companies, Walt Disney World has taken important steps towards building safety into its monorail system, both in systems design, and in procedural steps. However, this accident did occur. Perhaps there are some higher-level lessons learned regarding failure-free, safe operation, and how possible issues might be detected and avoided; lessons-learned for any such operation. Certainly, the reliability engineering profession uses tools designed to anticipate possible problems. But are they sufficient?

Fault Tree Analysis (FTA) and Failure Modes, Effects, and Criticality Analysis (FMECA) are both special tools that would be used in a high-cost, high-profile, people-intensive operation such as the WDW monorail system.

But what about the “one-failure-at-a-time” practice with these tools? It is common practice to review only one failure or mistake at a time. In most cases this is a reasonable assumption because the occurrence of two low-probability events at the same time is extremely small, and often considered a “rare event.”

In the case of the WDW monorail accident (and many other similar catastrophes), more than one “fault” occurred at the same time. So, is this a case of a one-in-a-million occurrence? This event is the first fatality in some 39 years of the monorail operation at WDW. Or was it just luck that this event was avoided for so long?

The multiple “faults” that had to occur to allow this accident to happen are outlined next.

- The first train was in position to back-up, but the operator failed to throw the switch, yet thought he had, and radioed that it was switched.
- The first train backed-up without knowing the tracks had not been switched, so he was backing down the main track, and not onto a spur, as intended.
- The second train came forward, but did not know the first train was not off the tracks yet, and the MAPO system had been disabled to allow the reverse operation.
- The replacement Central Coordinator did not see any missteps because he was at dinner.

Then, consider whether or not the fact that these four events occurred at one fatal moment is a “rare event.”

The first point, that the operator failed to throw the switch AND radioed that he had, might be considered a very unlikely occurrence. Throwing a switch is a physical act, likely to register whether or not it occurred.

What about the second point? There is no direct visibility by the pilot in front to see if the switch has been thrown or not, at least until the length of the train has passed the switch. So this event might be quite likely.

The MAPO system was in-place to detect a train too close, and to change the lights from green to yellow to red. But per standard procedures, this system was overridden to allow the backing maneuver of the first train to occur. Then, it would not be surprising if the second train did not know of the first train’s presence. It was 2:00 AM, and the MAPO system was disabled. So this, too, might be considered likely to occur.

The final point, that the Central Operator was not present to over-see the operation, was not a required part of the procedure. It was permissible for that operator to be away for short instances. This then is not an unlikely event, either.

So one unlikely misstep, the operator thinking he had set a switch that he hadn’t, combined with three reasonably likely occurrences, resulted in this catastrophe. This series of facts conflicts with the “rare event” assumption. Indeed, when conditions are right, the analyses must account for more than one incident.

Is it reasonable to suggest that all possible combinations of events be considered for an entire FMECA or fault tree? Probably not. For a large, complex system such as the monorail system, the number of possible events and associated causes are innumerable. Trying to consider all of them in combination could be more costly than the project or system itself. But what if ground rules are considered that would allow certain types of conditions to be considered?

a. Change the Ground Rules

Ground-rules could be established to assure these points are given weight without being time or cost prohibitive. For instance, the three “likely occurrences” mentioned above could be considered *conditions* over time, as opposed to *instantaneous* events. The botched switching is an event, the fact that the train operators thought the switch had occurred is more of a condition. Then the likelihood of operators’ perceptions intersecting with other events or conditions are much greater than just a one-shot occurrence. In other words, time becomes a factor.

As an illustration, take another unrelated example: a circuit-breaker that has failed short. In this case, it is indeed a failure, but it will exist as a condition until it is discovered, either by test or by need. So if a short to ground occurs in the circuit, then the circuit-breaker would fail to clear, causing a much greater event than expected. Or take the case of an emergency switch that doesn’t work. It is not the time to discover the failed switch when the “emergency” occurs. That time is too late!

So one specific ground rule in performing FMECA could be:

*For failures that, based on their nature, are not events, but conditional or chronic, must be considered along with related possible failure conditions in a FMECA.*

Likewise, in the performance of FTA:

*For chronic conditions that are not failure events, the probability of failure is not alone considered, but also the probability of that failure being present when related events could occur.*

Another concern from review of the monorail catastrophe: although, the corrective action of an additional spotter was implemented, other solutions should be considered. The added spotter improves the safety to the system. However, this is still a procedural “fix.” Thought should be given to other solutions, if not already done, such as an addition of television cameras, or at least speed monitoring, so that all involved have a clear picture of what is occurring, even with the MAPO disabled. So another ground-rule for safety analysis is

*give priority to physical safety features over procedural ones, especially when safety is involved.*

These rule changes could lead to a more effective approach to making design or procedural changes. This result leads to the second point, a legacy of decision-making.

b. A Legacy of Decision-Making

One of the ideas that seemed rather critical in this review was to utilize a spotter for trains in reverse. This point was made quite emphatically by the manufacturer, Bombadier, Inc. But in the 20 years after the monorail was completed, and the manual was written, it had become common practice to depend on the built-in monitoring system that was in-place in the system.

Trever Kletz, an expert on industrial accidents, noted while discussing industrial accidents [3] that

*“Organizations have no memory; only people have memories and they move on. After about ten most of the staff on a plant have changed. No one can remember why equipment was installed or procedures introduced and someone keen to cut costs or improve efficiency,... asks, ‘Why are we following this time-consuming procedure?’ or ‘Why are we using this unnecessary equipment?’ No one can remember, and the procedures may be abandoned or the equipment removed.”*

Of course, this is an exaggeration to make a point. Many good precautions in both equipment and procedural design are put in place for good reasons. These precautions are typically well-documented, and followed, until someone wishes to “update” or “simplify” them. The point is that sometimes, even with steps well-documented, the reasons for them are lost. Here are some specific ideas on how corporate memory might become more useful.

- Track past incidents and events. Sometimes some rather innocuous occurrence could provide insight into why certain checks and balances are in-place. These “lessons learned” should be documented.
- Often the reasons for specific safety precautions are found in the original FMECAs and FTAs performed during the initial phases of a project. Keep them, and use them.
- Given the myriad of paperwork and reading material that exists in a company, another key point is to use word-of-mouth. Meetings or discussions, reviewing past events or how an occurrence could have been more severe, could help to enlighten, and remind personnel of the need for precautions.
- Another key point from Mr. Kletz [3]: “Never remove equipment or stop following procedures unless you know why they were introduced.”

If these points are instituted rigorously, this would help the organization “gain” a memory.

## 5. CONCLUSIONS

Two key findings resulted from this study.

- a. **Update the ground rules of FMECAs and FTAs to assure chronic conditions are considered when developing safety precautions.** These types of analyses are typically excellent resources for the “why” of the precautions instituted. They should be summarized, and made easily available to operations, and design personnel alike.
- b. **When considering changes to established precautions, assure the reasons for those steps are known so that wise decisions can be reached.** This finding means that safety training or meetings should be held that not only review the standard practices, but the “why’s” as well. The event histories of specific equipment make excellent material for bringing such lessons home to the participants.

This paper utilized the Walt Disney World monorail accident that occurred in July, 2009, to review what steps had been taken to prevent such an occurrence. These steps were meaningful to assure passenger and employee safety throughout the system. However, these safety barriers were “broken” when that event occurred. If this event can happen to a large, well-established company like Walt Disney World, it can probably happen almost anywhere. This event, then, made an excellent example to illustrate how difficult it can be to avoid catastrophe, and every company must always be diligent in reviewing its safety rules and designs to assure all that can be done is done.

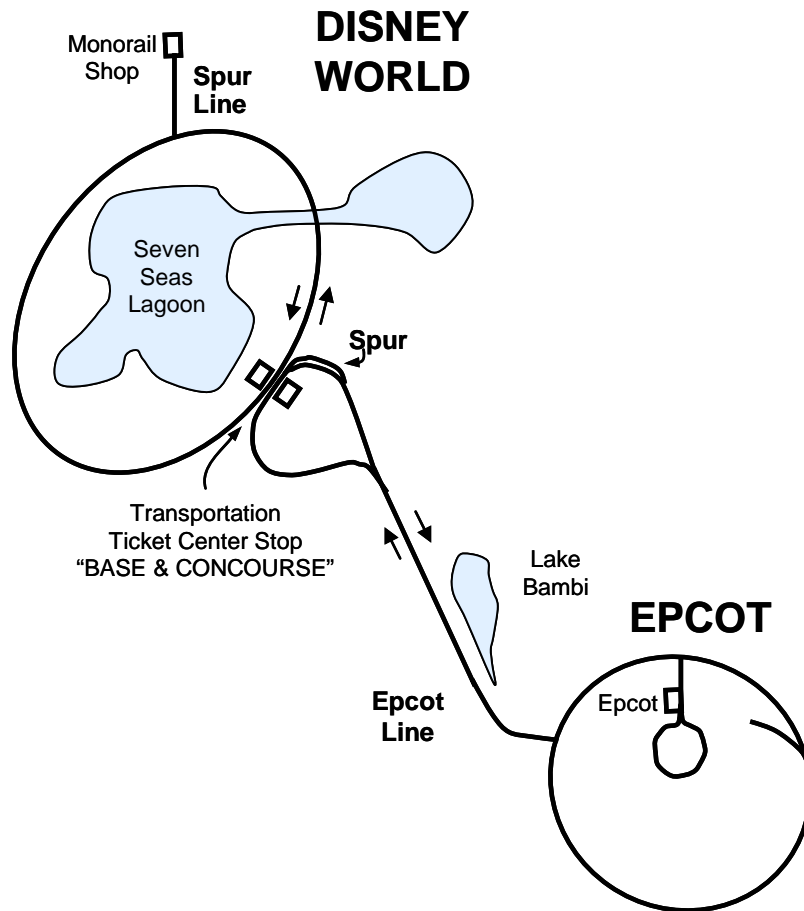


Fig. 1. A Layout Sketch of the WDW Monorail System.

### References

- [1] Orlando Sentinel, 07-29-2009, "Federal Investigators Now Reviewing Corporate Records as Part of Disney World Monorail Probe," Jason Garcia, Sentinel Staff Writer
- [2] Orlando Sentinel, 12-21-2009, "Monorail Guide Warned of Hazard When Trains Backed Up Without a Spotter," Jason Garcia, Sentinel Staff Writer
- [3] Lessons from Disaster – How Organizations Have No Memory and Accidents Recur," Kletz, Trever, Gulf Publishing Co., Houston, TX, 1993