National Aeronautics and Space Administration

SYSTEM FAILURE CASE STUDIES

APRIL 2009 *VOLUME 3 ISSUE 03*

Red Light

During London's morning rush hour on October 5, 1999, a commuter train passed a red signal and collided with a High Speed Train at Ladbroke Grove Junction. Thirty-one people died in the crash and subsequent fires. Although the incident could be attributed to driver negligence—all available safety features were functioning properly, and there were no technical or mechanical problems—the Health and Safety Executive investigation saw the incident as a "system-wide failure." Careful consideration in design of the human-machine interface and associated training may have prevented the collision.

BACKGROUND

RAILROAD TRAFFIC SIGNALS

British railroads employ a 4-aspect signaling system. The colors are familiar from traffic signals: red means stop at the signal, green means continue, and yellow stands for caution. The fourth aspect, a double yellow, was introduced to prepare high speed trains for an upcoming yellow signal, giving drivers advanced warning of a stop down the line. For trains traveling at lower speeds, a double yellow simply means proceed with caution.

A red aspect is also known as "danger"; when a train runs a red light, signalers refer to the incident as a "signal passed at danger" (SPAD). The critical signal in this incident, Signal 109 (SN109), is one of British Railways' top twenty-two most dangerous signals. There were seven SPADs at SN109 in the five years before the incident took place.

There are multiple signals at any given junction, generally one signal for each track. SN109 was one of six signals on a signal gantry.

TRAIN PROTECTION SYSTEMS

Automatic Route Setting: Signals were controlled by a Solid State Interlocking (SSI) system that used an Automatic Route Setting (ARS) program to assign routes according to a pre-determined timetable. The SSI and ARS ensured that routes did not overlap, preventing two trains from being assigned to the same section of track at the same time.

Automatic Warning System: Both trains involved in the collision carried an Automatic Warning System (AWS) to alert drivers to upcoming signals. As a train approached a red or yellow signal, the AWS sounded an audible alarm in the cab. If the driver did not push a button to acknowledge the warning, the AWS applied full brakes to stop the train. However, the driver could cancel the warning. If the driver canceled the warning, the AWS would not stop the train, even if it passed a red signal. The driver would have full control of the train.

Figure 1: The collision at Ladbroke Grove Junction

Train Protection and Warning System: The British Railway System was in the process of adding a Train

October 5, 1999: two commuter trains collide during London's morning rush hour, killing 31 people and injuring many more.

Proximate Cause:

- A diesel train (the 165) passed a red signal into the path of an oncoming high speed train, resulting in a nearly head-on collision.

Underlying Issues:

Weaknesses in the human-machine interface led to the collision:

- There were no engineering controls to protect against human error.
- Alarms did not distinguish between minor warnings and critical events.
- The driver could override the automatic train protection system designed to prevent Signals Passed at Danger (SPADs).
- Both the driver and personnel in the signal control room had inadequate training and experience.

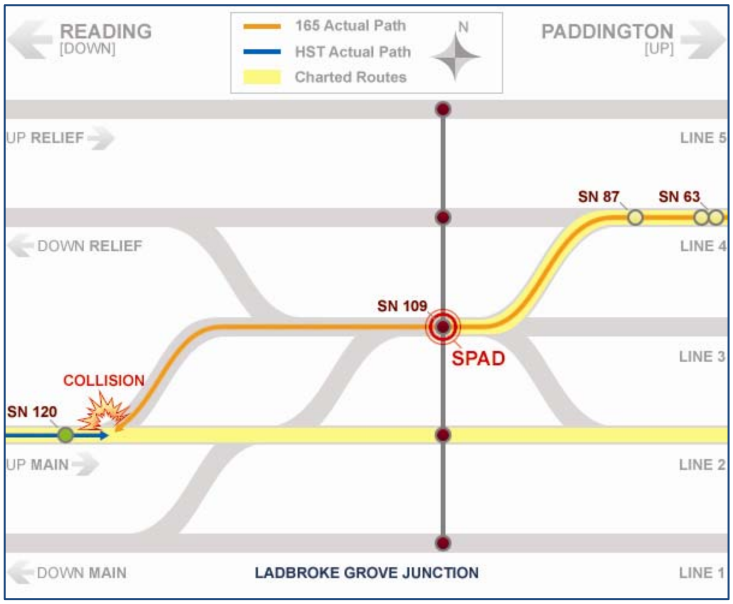

Figure 2: Diagram of the collision site

Protection and Warning System (TPWS). The TPWS design uses an on-track transmitter placed adjacent to a signal that is activated when the signal is red. If a train tries to pass the red signal, the TPWS activates the emergency brakes. SN109 was to be fitted with a TPWS before 2004, but the new system had not been installed when the incident took place in 1999.

What Happened?

On October 5, 1999, the High Speed Train (HST) 1A09 was carrying eight passenger cars eastbound towards Paddington on the main "up" line from Reading (Figure 2). The Automatic Route Setting gave the HST green signals along its route, giving it the right of way and a "full speed ahead" status.

Meanwhile, the slower Thames Train 3-car Turbo Class 165 (henceforth the "165") was bringing commuters "down" from Paddington. The ARS routed the 165 from Line 4 to Line 3 and then scheduled a stop at SN109 so the train would not collide with the HST (Figure 1). Prior to moving from Line 4 to Line 3, the 165 passed a double yellow at SN63, then a single yellow at SN87, which indicated that the next signal (SN109) would probably be red. Data recorders recovered from the train after the collision show that the driver correctly reduced power at the double yellow (SN63) and coasted through the single yellow at SN87. Instead of continuing to brake for the upcoming red at SN109, he increased power 239 meters before the signal. He then cancelled the AWS warning and passed SN109 at danger.

Signal Passed at Danger

The driver did not slow down after passing the signal. Relatively inexperienced, he probably did not realize that he had moved onto the wrong track—the Up Main Line. He finally applied the emergency brakes when he could see the oncoming HST, but it was too late to prevent the collision.

At the control center, signalers did not immediately realize a deadly SPAD had occurred. An audible alarm told signalers that a track circuit was occupied "out of sequence" and a visual display showed that the 165 had passed SN109 at danger and was headed towards the approaching HST. When they realized what had happened, one signaler changed the next signal in the HST's path to danger (SN120), while another radioed a "STOP" message to the 165's driver. Neither driver had enough time to respond to these attempts to avert the collision.

The Collision

The 165 was traveling at just under fifty miles per hour when it collided with the HST, which had been traveling at approximately eighty miles per hour. The steel HST pushed through the first coaches of the aluminum 165, which disintegrated on impact. As the HST penetrated the 165, it ruptured a fuel tank in the 165's leading coach. A cloud of diesel fuel ignited and started fires in several cars.

Thirty-one people died in the collision and resulting fires, an additional 227 were taken to the hospital, and 296 were treated for minor injuries on site.

Proximate Cause

A diesel commuter train (the 165) passed a red signal at Ladbroke Grove crossing. It continued approximately 700 meters into the path of the approaching high speed train before the two trains collided with a closing speed of approximately 130 mph.

Underlying Issues

Critical failures in the interface between humans and machines led to the Ladbroke Grove collision. No evidence was found of mechanical failures in the track, in the trains, or in the existing train protection systems.

There was also no evidence found of factors influencing the driver's performance such as distractions in the cab or malicious intent on the part of the driver. Human factors experts discounted inattention or fatigue, because the train had left Paddington Station less than three minutes earlier. Although it is impossible to entirely rule out such factors, the board looked for other explanations. Based on the driver's behavior as he approached SN109, the board speculated that the driver went through the signal because he believed it was yellow.

The leading theory about the accident was this: because the driver could see all the other signals were red, he concluded SN109 showed a "proceed" aspect. His driving pattern supports this hypothesis: after coasting through the yellow at SN87, he increased speed at the point where all the signals on the gantry except SN109 were visible.

Signal Layout

SN109 was one of several signals on the gantry, but it only became fully visible approximately 60 meters after the other signals. The investigation concluded that drivers were faced with "an exceptionally difficult signal reading task" at SN109. On approach, the gantry was frequently obscured by transverse girders and overhead line equipment, making it difficult to get a clear view of the signal. The complexity of the gantry layout further added to the challenge of discerning SN109 from the other signals.

Human-Machine Interface

The Automatic Warning System on the 165 used the same audible and visual warning to notify the driver of either a yellow or a red signal. The driver cancelled the AWS warning as he approached SN109, an automatic response for drivers who are aware of the situation and can either stop the train or proceed under their own control. However, the driver may have assumed it had a yellow aspect. The interface did not provide distinction to reduce the likelihood of human error.

Figure 3: A complex railway junction (not SN109).

Just as the AWS did not distinguish between signals, the Automatic Route Setting used in the control room did not have a unique alert for SPADs. Instead, a single, brief "tweet" indicated that something required a signaler's attention. Once they heard the alert, signalers had to use a variety of displays to determine what had happened and how to respond. Approximately eighteen seconds after the SPAD, signalers radioed a "STOP" message to the 165 and changed SN120 to danger. The investigation estimated that they would have had to send the signals within fifteen seconds to give the drivers enough time to stop the trains. Again, the human-machine interface was not designed to minimize error and improve efficiency.

Training and Experience

The 165's driver had completed his training only thirteen days before the incident. A review of the driver training program had recently identified weaknesses in training such as lack of course structure and consistency, lack of training validation, and insufficient attention to SPAD prevention. Several recommendations came from this review, but the recommendations had not yet been implemented when the 165's driver was certified. Inadequate training and driver inexperience almost certainly contributed to the driver's errors.

Training in the control room was also found to be inadequate. Instructions contained direction on procedures in the event of a SPAD, but signalers had no opportunities to practice responding to SPADs. They were only trained if they happened to be on shift when an actual SPAD occurred.

Systems and Human Error

The United Kingdom was one of the last countries in Europe to run high speed trains and mixed traffic without modern train protection systems. The 165 train was scheduled to be fitted with a Train Protection and Warning System (TPWS), a capture control which would have identified the SPAD at SN109 and applied the train's braking system. Although studies have uncovered several reliability and effectiveness concerns with TPWS, the investigation board concluded that in this case the TPWS would have prevented the accident. Without the TPWS, human action—or inaction—had fatal consequences.

Aftermath

Ladbroke Grove was one of a series of similar rail catastrophes in Great Britain. The accident sparked several public inquiries to provide recommendations for improving safety in British railways and investigate broader questions regarding train protection and warning systems. One recommendation resulted in the formation of the Rail Safety and Standards Board (RSSB). Since its inception in 2003, train accidents with potential for serious consequences have fallen dramatically. SPADs have decreased by more than ninety percent, and fatality rates on British trains are now at their lowest ever, with an average of less than one death yearly. The RSSB continues to develop and implement risk management tools to enhance rail safety.

Applicability to NASA

Work at NASA is very different from the routines of the railroad, but this incident brings out several critical principles for successful NASA missions.

Human Capabilities and Limitations

Considering human capabilities and limitations in system design reduces the risk of human error and allows for the development of safer systems. Errors are more likely when interfaces are complex or cluttered; a simple display is usually more effective than an interface that communicates a lot of information all at once. In the control room, signalers had to sift through multiple displays to locate the SPAD. The alarm that alerted them to the problem did not distinguish between minor warnings and critical events, so they did not immediately send out an emergency stop signal. Similarly, SN109 was on a complicated gantry that was notoriously difficult to read.

Effective training enhances human capability. SPAD prevention was particularly important for small commuter trains, which were frequently required to stop at red aspects to allow larger, faster trains to pass, yet emphasis on this

Questions for Discussion

- Do you use engineering controls to minimize the need for human action or conscious effort?
- Within your specific project, how can you improve designs to minimize the effects of human error?
- Does your team report high severity close calls and investigate and address root causes prior to resuming operations?
- Do alarms you work with provide a logical warning progression? Are control measures sometimes ignored because they are frequently innocuous?
- Does your training provide an opportunity for personnel to become proficient in necessary skills?

element varied by instructor. Effective training would have consistently addressed this essential responsibility.

Skill development through experience also improves the likelihood of successfully performing expected tasks. The driver of the 165 train had only been on the job for thirteen days. Additional experience and historical knowledge may have helped him respond to the signaling differently.

Human Expectations and Logic

Humans tend to develop expectations based on past experience. This can be used to develop safer systems, but it can also have a negative effect when systems are not designed logically. The AWS alarm did not distinguish an upcoming red aspect from a yellow aspect. Effective alarms and warnings differentiate between degrees of severity, and effective displays prioritize critical information. The aspect signaling did not necessarily follow a standard sequence. Consistency in warning progression is a normal human expectation. When approaching a traffic signal while driving, we expect a red light to follow a yellow light.

Repetition is a natural part of skill development through on the job training. The proper actions become second nature. Unfortunately, negative behaviors can also become second nature. If an AWS signal sounds, an experienced driver's first action may be to override the alarm, then individually assess the situation, because that is how it has always been done. This action could allow the operator to focus better on assessment, but it might also reinforce behavior to ignore a hazard.

Reliance on Human Action

At Ladbroke Grove, human initiative overruled the Automatic Warning System. An effective system would not have allowed a driver to pass a red signal. Engineering control measures can be designed into a process so that no human action or conscious effort is required. At NASA, engineering controls with built-in redundancies are employed in safety-critical situations.

However, in some situations it is necessary to rely on humans to effectively interface with machines. Humans are sometimes needed to adapt to unexpected or unique situations, or to follow a logic path outside a machine's capability. When this is necessary, it is critical to apply sound human factors solutions to aid human performance. The human-machine interface must consider human capabilities and limitations, human expectations and logic, and performance shaping factors. Streamlining the human-machine interface can reduce the risk for errors in perception, data interpretation, decision-making, and action execution.

References

Chandler, Faith. *Introduction to Human Factors in Mishap and Close Call Investigations.* NASA training course. Accessed 26 January 2009. <http://satern.nasa.gov>

"How the accident happened." BBC News-World Edition. 8 October 1999. Accessed 19 January 2009. <http://news.bbc.co.uk/2/hi/uk_news/469038.stm>

"Paddington Signal Back in Service." BBC News. 12 February 2006. Accessed 19 January 2009. <http://news.bbc.co.uk/1/hi/uk/4705696.stm>

"Railroad." Encyclopedia Britannica Online. 2009. Accessed 06 Jan. 2009 <http://www.britannica.com/EBchecked/topic/489715/railroad>

Rail Passenger Safety. Safe Trains Action Group. 29 Aug 2001. Accessed 30 Dec 2008 <http://www.macro.org.uk/rail-safety.htm>.

Rail Safety and Standards Board website. RSSB. Accessed 19 January 2009. <http://www.rssb.co.uk/>

Rush, Jonathan. "Len Porter Rail Safety and Standards Board." Contingency Today. 30 January 2007. Accessed 19 January 2009. <http://www.contingencytoday.com/online_article/Len-Porter-Rail-Safety-and-Standards-Board/47>

"The Ladbroke Grove Rail Inquiry, Part I." The Rt Hon Lord Cullen PC, HSE Books. 2001. Accessed 06 Feb 2009. <http://www.rail-reg.gov.uk/upload/pdf/incident-ladbrokegrove-lgri1-optim.pdf>

"The Ladbroke Grove Rail Inquiry, Part II." The Rt Hon Lord Cullen PC, HSE Books. 2001. Accessed 06 Jan 2009. <http://www.rail-reg.gov.uk/upload/pdf/incident-ladbrokegrove-lgri2.pdf>

"The Train Collision at Ladbroke Grove 5 October, 1999." A Report of the HSE Investigation 2000. Accessed 30 Dec 2008 <http://www.rail-reg.gov.uk/>.

Uff, Professor John, QC FREng, and the Rt Hon Lord Cullen, PC. *The Joint Inquiry Into Train Protection Systems.* 2001. HSE Books. Accessed 30 Dec 2008. <http://www.rail-reg.gov.uk/upload/pdf/incident-ladbrokegrove-jointinquiry.pdf>

Acknowledgements:

Special thanks to Dr. Barbara Burian for her insightful peer review.

SYSTEM FAILURE CASE STUDIES

NASA SAFETY CENTER

Executive Editor: Steve Lilley steve.k.lilley@nasa.gov
Developed by ARES Corporation