The Contribution of Degraded Modes of Operation to Accidents in the US, UK and Australian Rail Industries

Chris. W. Johnson, DPhil; Department of Computing Science, University of Glasgow, Scotland, UK.

Christine Shea, PhD; ESR Technology Ltd, Birchwood Park, Warrington, Cheshire, UK.

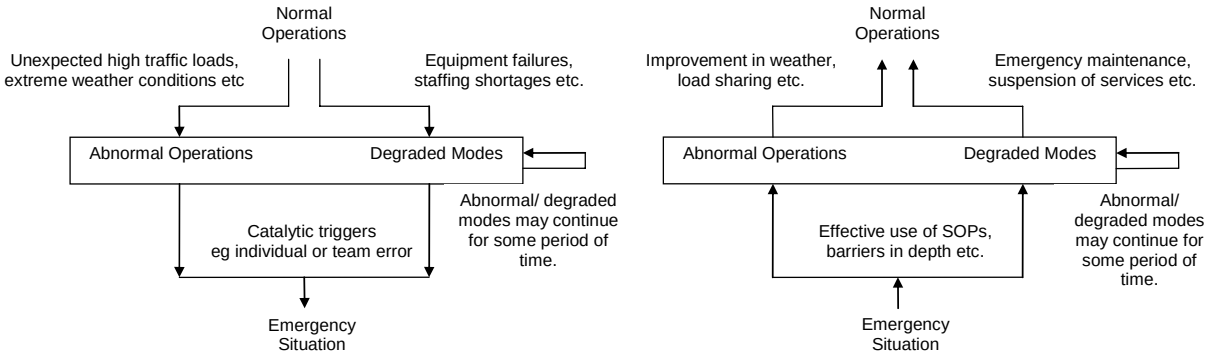
Keywords: rail transport; degraded operations; accident analysis; derailments.

Abstract

Degraded modes of operation occur when technological systems fail to meet the levels of service that are expected by staff and managers. Over time, operators develop 'work arounds' that help them to cope with these degraded modes. This has led to a culture of 'making do' where co-workers try their best to maintain service provision in spite of system failures. The extent to which operators will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, these adaptations and 'work arounds' undermine safety. A central aim of this paper is to identify and begin to understand why teams of co-workers continue to operate safety critical systems when key elements of their infrastructure have been compromised, for example during routine maintenance.

Introduction

Many accidents and incidents occur during 'degraded modes of operation'. They happen at times when operators cannot rely on the supporting infrastructure that is otherwise available under 'normal' conditions. For example, the UK Railway Group Standards [1] contains the following distinctions. **Normal operations** describe the way in which the railway was designed to operate, including planned peak periods. **Abnormal operations** arise from extreme loading on a part of the railway system, for example as a result of severe weather, or delays to a train service impinging on others. **Degraded operations** occur when part of the railway system continues to operate in a restricted manner, for example after the failure of signals. **Emergency situations** include an unforeseen or unplanned event which has life-threatening or extreme loss implications and requires immediate attention, for example a fire, or an obstruction on a line. Figure 1 illustrates key relationships between these different modes of operation.



a) Transitions towards emergency situations

b) Transitions towards normal operations

Figure 1 — Overview of Degraded Modes in the Transition to Emergency Situations

It can be difficult to define the precise characteristics of normal and abnormal operations both within and between rail systems. For example, European states disagree about the list of equipment that should be available to support drivers/engineers under normal operating conditions. We, therefore, face a situation in which it is difficult or

impossible to develop minimum equipment lists that might be used to characterise routine operations across national and international rail networks. Rather than extend the existing debate in this area, the following pages focus instead on the problems that arise during degraded modes of operation. We focus on three case studies from different rail systems. The Glenbrook collision occurred in New South Wales, Australia [2]. An interurban passenger collided with the rear of an Indian Pacific long distance passenger train that has slowed after reaching a failed signal. A number of factors were involved, from equipment breakdown to poor phrasing of the rules and to deeper issues to do with the safety culture in rail operating organisations within New South Wales. Seven people were killed in the accident.

The second case study focuses on the Southall rail crash [2]. A First Great Western InterCity passenger train from Swansea to London Paddington, operating with a defective Automatic Warning System (AWS), went through a red signal and collided with a freight train leaving its depot. The AWS provides advice to the driver and so might have alerted them to the danger had it worked as intended. The train was also fitted with an Automated Train Protection (ATP) system but this was switched off. The driver was initially charged with manslaughter but the case was dropped. Great Western Trains was fined £ 1.5 million for not having a system to ensure that high speed trains were protected by AWS over longer journeys. Six people were killed and over 150 were injured.

The third case accident occurred when a westbound Northeast Illinois Regional Commuter Railroad (Metra) train derailed its 2 locomotives and 5 passenger cars as it traversed a crossover between 2 tracks in Chicago, Illinois [3]. The maximum authorized speed through the crossover was 10 mph, however, it was later determined that the train had derailed at around 68 mph. A number of safety issues were identified in the aftermath of the accident including the locomotive engineer's performance, training, and qualifications. As a result of the derailment, 47 passengers attended local hospitals. 44 were treated and released, and 3 were admitted for observation. Damages from the accident exceeded $5 million.

High Level Management Priorities and the Pressure for Service Continuity

Management priorities play an important role in creating the context in which degraded modes of operation are likely to occur. Organisations often place undue emphasis on operational priorities that persuade staff to continue service provision even when safety is jeopardised. For example, the Glenbrook report makes many references to a 'culture of on-time running' that existed at the State Rail Authority of New South Wales [2]. The concern to meet the timetable deadlines led to drivers being forced to operate trains without functioning radios or with defective brakes. The implications of this concern for 'on time running' are spelled out in later sections of the report "degraded modes of operation accidents are more likely to occur, particularly if employees acting under the imperative of on time running are trying to have the infrastructure perform more efficiently than it is capable of doing" [2, p.150]. In other words, by placing undue emphasis on meeting the timetable there is pressure to underreport equipment failures and delay remedial actions. Not only does this undermine safety but in the longer term will lead to greater inefficiency across network operations.

Similar pressures to meet operational targets also affected events leading to the Southall collision [3]. Signals SN280 and 270 were intended to provide the driver with sufficient warning about the hazards posed by the freight train as it crossed in front of the high-speed train. However, it can be argued that the decision to route the freight service in front of the passenger train was a contributory factor in the eventual accident. Railtrack, the infrastructure operator, had been responsible for introducing a new regulation scheduling policy in 1996 based on minimizing overall delay. The train operating companies were expected to meet Track Access Conditions that referred to the protection of 'commercial interests' [3, p.78]. This was partially driven by rail privatization. No risk assessment was conducted to consider the consequences of these provisions nor was there any similar analysis of the ARS automatic signaling system that embodied these requirements.

Links Between Training, Safety Culture and Degraded Modes of Operation

The Glenbook investigation team argued that poor training was compounded by the lack of an appropriate safety culture and that this created the context in which degraded modes of operation are more likely to cause accidents: "Many accidents occur during what is described as a degraded mode of operation, that is, when normal operations are disrupted for one reason or another, such as an infrastructure or rolling stock failure. It is at such times, as the

Glenbrook rail accident itself demonstrated, that the risk of accidents is increased if the procedures or training are inadequate or if there is a lack of an appropriate safety culture" [2, p. 43]. In particular, the driver of inter urban train, Mr Sinnett, "did not appear to have proper training in the operation and effect of safeworking unit 245". Safeworking units described the approved means of working under a number of operating conditions. Unit 245 specified that extreme caution should have been used after passing an automatic signal at stop. The implication being that such caution would have enabled the interurban train to stop before colliding with the rear units of the Indian Pacific train. However, the particular actions of the train crews are often caused by underlying or latent problems in the safety management systems that create the context for accidents that occur under degraded modes of operation. ***Problems in training did not create the degraded modes of operation but may have prevented the engineers or drivers from responding to mitigate failures that were associated with these degraded modes***:

The argument that inadequate training left operating staff vulnerable to the problems created by degraded modes is repeated in the Southall accident report. A technical failure in the Automatic Warning System (AWS) left Driver Harrison without an important reminder of the aspect of the signaling system. At the time of the accident, there was some debate within the industry about the status of this system. Many felt that it provided additional reminders to the driver and so should be viewed as a driver aid and not an essential safety-related system. In consequence, the driver had never driven a high speed train without AWS nor had he received any training on what to do without such support. Similar comments can be made about the lack of training that was cited as a reason why the driver was prepared to operate the train without operating the Automatic Train Protection (ATP) system that was installed on the unit. At the time of the accident, ATP training was not part of the operating company's system for Driver Competence Assessment. Hence it was entirely possible for a driver to operate a High Speed Train without feeling competent to operate the ATP equipment. This reflects the manner in which corporate policy influenced the behavior of individual drivers. For example, the company had no system for matching ATP competent drivers with ATP designated services [3, p. 55].

The Importance of Maintenance in Degraded Modes of Operation

Maintenance has a profound impact on degraded modes of operation. For example, the passenger train involved in the Southall collision was operating without AWS. This fault has been reported on the day before the accident. However, the Maintenance Depot could not replicate the fault and the train was passed for service. The AWS functioned normally during the ten minute drive from the Old Oak Depot to Paddington station. However, on arrival Driver Tunnock found that he could not cancel the warning system. He isolated the AWS to release the brakes and reported the problem to the Operations Supervisor at Paddington. He also informed the operating company, GWT, by telephoning the Control Center at Swindon. The official investigation records that GWT Control either "overlooked or lost both this message and a further one sent by Driver Tunnock from Swansea... Fitters were called from the GWT Landore Depot attended the train at Swansea but did not attempt to repair the AWS. GWT took no action to withdraw the train from service" [3, p. ii-iii]. In retrospect, it seems difficult to explain why the service was allowed to continue once maintenance and service personnel had been alerted to the problem. However, it is important to recognize that railway operations often continue in the presence of background faults. This makes it difficult for maintenance staff to accurately judge 'borderline' failures; it is a non-trivial task to accurately distinguish those failures that directly threaten safety from more 'normal' problems which need not affect continued operations. For example, the High Speed Train suffered from a number of other faults in addition to the loss of AWS. The buzzer used to support communications between the driver and guard was not functioning correctly. By convention, the guard provided two short buzzes to inform the driver that the train was ready to depart. However, the buzzer was sounding continuously at the rear of the train and did not work at all in the front. As suggested in previous sections, such 'normal failures' led to the development of coping strategies; platform staff either illuminated an indicator for the driver to depart or pass the guard's signal to the driver. This use of coping strategies to deal with 'background' or normal failures can be seen in other aspects of the Southall accident. For example, the initial driver of the High Speed Train tried to inform the subsequent driver that the AWS system had been isolated. This would usually have been done through the fault repair book in the cab of every power unit. However, this was already full and so the driver fixed a note to the dashboard stating "AWS ISOLATED REPAIR BOOK FULL" [3, p.3].

The Glenbrook report revealed a background of problems in the coordination of maintenance activities. These included a fatal accident where trackside workers failed to consider the possibility that trains would pass close to

them on the other track. Hence the lookouts were not placed in positions that would warn workers when trains were approaching in the other direction from the section that they were working on. In this example, the maintenance team were addressing an infrastructure failure that led to degraded modes of operation by restricting traffic on one of the lines – the official report argues that engineers failed to consider adequate restrictions; "the first question they should be asking themselves is whether it is reasonably feasible for trains to be stopped entirely while the work is carried out so as to remove the risk of employees being struck by trains" [2, p. 50]. Many maintenance failures do not have such serious consequences. They lead to incidents that might have had far more severe outcomes. It is for this reason that the Glenbrook report criticizes a number of background problems. For example, the sustained analysis of previous incidents looked at a derailment that took place at Hornsby in January 2000. Only one bogie of the leading car came off the rails and nobody was injured. One of the factors in this incident was the lack of a functioning speedometer on the train. The driver had to estimate their speed in order to determine whether or not they were meeting the speed restrictions on various sections of the route; "this is clearly an unsatisfactory state of affairs"[2, p. 104].

The Interaction between Operating Rules and Degraded Modes of Operation

Regulators and operating companies recognise the safety implications of 'degraded modes' and, typically, respond by drafting rules to guide operator intervention. However, it can be difficult to identify all of the possible problems that might restrict normal operations. It is, therefore, almost impossible to ensure that any regulations will adequately address the safety concerns that arise from these modes of operation. This is illustrated by the regulations governing maintenance on the Automatic Warning System (AWS) prior to the Southall collision. In 1980, the former unified authority, BR, issued specification MTf169 which stated that the vehicle should be returned to traffic if it passed the tests that were performed on the high speed train on the night before the accident. However, in 1989 a further regulation was issued. TEEICM/89/M/200 required that after a successful magnet test all items of the AWS should be examined and a 'test box' used before the vehicle was returned to normal operations. The drafting of the new regulation created some confusion because the intended incorporation of the two specifications never took place [3, p.67]. Similar ambiguity is apparent in the rules governing degraded modes in terms of train operation with a failed AWS. The isolation of this system is addressed in the drivers' Rule Book that governed operations at the time of the Southall accident. Appendix 8 states that **"**A traction unit must not enter service if the AWS is isolated or the seal is broken on an AWS isolating handle in any driving cab which is required to be used… If it is necessary to isolate the AWS the driver must inform the signalman at the first convenient opportunity. The train must be taken out of service at the first suitable location without causing delay or cancellation". It is unclear whether the train should be kept in service if delay or cancellation would otherwise be caused given that some interruption to normal service would occur unless a replacement train was immediately available. Alternatively, the use of the word 'must' could be taken to indicate that the unit should be taken out of service whether or not it led to delays or cancellations [3, p.143].

The rules governing degraded modes of operation also played a significant role in the Glenbrook accident. The operational rule known as 'safeworking unit 245' required that a driver must proceed with extreme caution if they had obtained authority to pass an automatic signal at stop. In this accident, a power supply unit failed. This provided electricity to a train sensing circuit within the automated signaling system. The circuit overlapped to blocks of track and so caused two consecutive signals to 'fail safe' with a stop or red indication. As required by unit 245, the driver of the Indian Pacific train obtained permission to proceed onto the next signal after the initial stop indication. The driver was concerned by the second red signal and so got out to use the signal post telephone. Again in accordance with the safeworking unit, he wanted to obtain further permission from the signaler to continue beyond the second signal. However, as mentioned previously, he failed to contact the signaler erroneously believing that the phone would not work because the 'press to ring button' was broken. He, therefore, returned to the locomotive and following the provisions of unit 245 waited for a further minute to enable any trains ahead of his unit to clear the next section of track. This delay was unnecessary because the stop aspect was caused by the fault rather than the presence of another train on the section. However, the additional delay reduced the headway between the Indian Pacific unit and the following inter urban train. The signaler told the driver of the inter urban train that he could "just trip past it". However, he continued to obey regulation 245 and requested permission from the signaller to pass; "I'm right to go past it am I mate?" elicited the response "Yeah, mate, you certainly are". The official report argued that the colloquial nature of this exchange gave the inter urban driver the false impression that

the track ahead was clear. The driver proceeded beyond the signal and was traveling at approximately 50km per hour when he saw the rear of the Indian Pacific train but was unable to avert the collision [2, p. 10].

The Chicago accident also reveals important interactions between regulations and degraded modes of operation. The Federal Railroad Administration introduced Emergency Order No. 20 Notice Number 1 following 2 fatal train accidents. The order was aimed at commuter and intercity operations using multiple power units in a push-pull configuration in circumstances where there was no protection provided by 'cab signal, automatic train stop, or automatic train control systems' [4, p.12]. The notice covered situations where there were no cab signaling systems, similar to the UK AWS, which might remind crews when they pass a signal with a restriction. In such circumstance, the engineer should called out the aspect of the signal to a designated crewmember elsewhere in the train if it it was at, or less favorable than, 'approach'. The crewmember must then confirm the message. These special instructions were intended to provide significant barriers against crewmembers forgetting the aspect of signals. As we have seen, however, it can be particularly difficult to draft regulations that cover the diverse conditions that lead to degraded mode accidents. In this case, the operator's special instruction did not apply because the engineer did not need to communicate the aspect of the two signals before the derailment. These were given as 'approach diverging' and 'diverging clear'. Both of which are more favorable than an 'approach' signal indication [4, p.13]. Similarly, Emergency Order Number 20 allowed railroads to specify yard or terminal limits within which engineers were exempt from the requirement to call out signals to their colleagues. In the Chicago accident, the Metra terminal exemption extended beyond the derailment site to almost 4 miles from the station. The eight signals between the Chicago yard and the Root Street Tower were never called out, regardless of their indication, because they were within Metra's exempt terminal area. This exemption was justified because of the existing heavy volume of radio traffic needed to schedule train movements in the area. There was a concern that the additional calls/communications required by Emergency Order Number 20 would create confusion that could in turn compromise safety [4, p.13]. In other words, a concern over the human factors problems of additional communications led to an exception in the regulations, which in turn increased the complexity for engineers seeking to implement the operators' interpretation of the FRA requirements.

All three accidents illustrate the problems of continually revising operating rules to address the hazards created by degraded modes of operation. These regulations have become so complex that many 'front line' staff only have a minimal grasp of the procedures that they are required to follow. The official report into the Glenbrook accident quotes a driver's opinion on 'safeworking units'; "My view is that they have become largely irrelevant to the guy that is doing…the job because they are more of a library addition, rather than an actual workbook I can take with me. It is pretty hard to carry all those manuals on the job with you" [2, p.130]. In the aftermath of all three accidents, calls were made to improve drivers' understanding of the regulations that govern their interaction with degraded modes on their rail systems. Often these calls were made in spite of the observation that the rules and procedures were themselves flawed and would not have avoided the adverse outcomes.

Incident Reporting and the Movement towards Degraded Modes of Operation

Reporting systems help to ensure the detection of, and response to, degraded modes of operations. Drivers and engineers can exploit fault tracking systems to provide maintenance crews and management staff of problems with the operating infrastructure. Incident reporting schemes provide means of eliciting information about situations in which degraded modes help to undermine the safety of existing operations. However, management actions can undermine the 'reporting culture'. For example, the Glenbrook investigation revealed how a driver reported a defective signal that could not be replicated by a signal electrician. The driver was then charged with making a mischievous report. In another example, a driver/engineer was forced to continue operating a train even though he had filed a report to indicate that it had faulty brakes [2, p.45-6]. Such actions can dissuade colleagues from providing the information that is necessary if management and maintenance staff are to restore infrastructure components to normal modes of operation.

A central aim of this paper is to explain why staff try to maintain service provision even when they have significant concerns about the safety of their operations? The driver of the High Speed Train in the Southall accident, in common with other workers in the UK, had a general right to refuse to work in situations where they perceive danger, either to themselves or to others. The duty to report such circumstances is explicitly mentioned within the Safety Case that justifies the train operating company's operational arrangements. Part of the explanation lies in

the motivation of system operators to maintain service provision even under degraded modes of operation. After the Chicago accident, the engineer reported that he had a number of worries prior to the derailment. These included his uncertainty about the location of a maintenance-of-way crew working close to the line. The engineer was also worried about his approach to station platforms. He was driving engines that were significantly more powerful than any he had used before. However, his concern to meet operational expectations arguably motivated him to continue his scheduled tasks without seeking additional help [4, p.11].

The structure and organization of the railway industry can complicate the tasks that operational staff must perform when they report faults involving critical infrastructure components. The Southall accident occurred in the aftermath of rail privatization in the United Kingdom. One consequence of this was that drivers were employed by different organizations, the train operating companies, from the signalers who were employed by the infrastructure providers, Railtrack. If the driver informed the signaler of a potential problem, the signaler would pass the information via their reporting structures to Railrack Control whereas the driver would report to the Train Operating Company's Control center. Although there different control centers were in close contact, the different reporting structures that were a side-effect of privatization had not been reflected in structural changes to the associated reporting rules [3, p.145].

Human Factors and Operator Performance during Degraded Modes of Operation

NTSB investigators had to explain why the engineer's statement that he did not notice any potential problem until the train hit the crossover switch given that the diverging clear signal was discernable from around 7,900 feet before the crossover point. Part of the explanation lies in the background and training of the engineer. The engineer had worked on lines that generally used older, less powerful locomotives than the one that was involved in the derailment. These provided 3,200 horsepower compared to 3,600. There were further differences; the driver was used to single locomotive operations. On the day of the accident, he was using dual power units for the first time. After the accident, the engineer described how this configuration accelerated more quickly than he was used to. In consequence, he had to repeatedly check his speed and apply braking to compensate for the additional power. He stated that "[the new locomotives] go so fast, you could find yourself 5 to 10 miles above the speed limit if you're not paying attention". In addition, the controls on the newer locomotives were on a desktop stand rather than on a control plinth at the engineer's left-hand [4, p.11]. In consequence, the engineer's concern over the location of a track-side maintenance crew and the regulation of the train speed may have compromised his situation awareness. These preoccupations may have undermined his perception of signal aspects and his ability to react to them appropriately [4, p.17]. None of these issues stem directly from the problems of 'degraded mode operations' which lie at the heart of this paper. In contrast, they illustrate the converse situation in which enhanced functionality creates human factors demands that lead to emergency situations. This has important implications for our analysis. In arguing that reductions in operational performance create the preconditions for incidents and accidents, we must not forget that improvements in equipment provision also create the human factors demands that threaten safety unless adequate training and supervision are provided.

Automated systems play an increasingly important role in the human factors issues that arise during degraded modes of operation. The Southall accident provides numerous insights into the temptation to maintain levels of service in the presence of automated systems failure. Many drivers felt that AWS was merely an 'aid' rather than a central tool. However, the investigators believed that the accident emphasized the importance of AWS and undermined this view of the system as an additional extra that was not critical to many driving tasks. The idea that an automated warning system would continue just to be an 'aid' is also challenged by human factors research which suggests there is a tendency to rely on such tools the longer they remain in operation [5]. It was argued that 'a full understanding of the effect of such systems depends upon studies of human behaviour in the particular environment of the driving cab, a subject which has so far received only limited attention' [3, p.86]. One important aspect in the changing role of AWS was the gradual increase in operating speeds over the network. This combined with the use of interlocking systems and significant reductions in signaling errors has led to driver error increasing in prominence as a cause of accidents and incidents. Hence the importance of AWS had increased as a means of ensuring safety across the UK rail system. The significance of the system had not been reflected in the rules and regulatory procedures that governed operations before the Southall accident; as we have seen there were many instances in which trains continued to operate with AWS isolated.

Prior to the Southall accident, no risk assessment had been conducted for continuing operations without AWS. Had such an assessment been conducted then it might also have revealed the limitations of AWS. For example, the majority of signals passed at danger (SPADs) continue to occur with trains that are equipped with AWS. In such circumstances, drivers cancel the warning and proceed without applying the brakes [3, p.141]. The cancellation of Automatic Warning System (AWS) warnings can occur when drivers become habituated to the system, acknowledging warnings more as a reflex action than as a considered response to a potential hazard. This is unsurprising given that all drivers encounter many AWS warnings each day.

A number of different problems affect the implementation of Automated Train Protection (ATP) systems. Initial trials of the ATP systems on the section of track involved in the Southall collision suffered from problems of water ingress into the speed sensors that are attached to the axle end on the trailing bogie of power cars. Further problems arose from vibration failures so that a more robust version of the system had to be installed on rolling stock. This revised system suffered from problems in accurately measuring the distance that each train had covered. The software identified potential collisions with following trains when the system underestimated the distance that the lead train had traveled. In consequence, drivers were faced with a number of spurious emergency brake applications. Following the Glenbrook accident, it was revealed that ATP equipment was the greatest single item of maintenance on the Queensland system. Two subsequent train collisions in 1989 and 1994, stemmed in part from the installation of ATP; 'the first collision was brought about by the driver having insufficient air left within the braking system to apply the brakes on the train as the Swedish system had been bought off the shelf and had never been designed to cope with the problem of low air… the second accident in 1994 occurred because the driver kept overriding the system [2, p.154].

The media and the general public have urged the installation of ATP equipment as a means of guarding against driver/engineer errors of the kind witnessed in our case study accidents [2, 3, 4]. The general tenor of the public response can be seen in sections of the NTSB report into the Chicago derailment. They argued that accidents over the previous thirty years had shown 'conclusively' that positive train control systems such as ATP are the most effective means of avoiding train-to-train collisions [4, p.20]. Hence the introduction of these systems has been on their 'Most Wanted' Transportation Safety Improvements list since it was developed in 1990. In summing up their findings, the Safety Board concluded that a system similar to ATP could have prevented the Chicago derailment; 'such a system could have detected the engineer's lack of response to signal indications and then could have either stopped the train or slowed it to a speed at which it could have safely moved through the crossover… the Safety Board believes that Metra should install a positive train control system on its commuter train routes' [4, p. 22]. However, such comments ignore the maintenance and reliability issues that affect ATP applications. This is important because, as we have seen with AWS, there are significant consequences if operational staff become used to 'working-around' failed systems that might otherwise play a significant role in supporting their everyday tasks. The official investigation into the Glenbrook collision makes this point in a concise manner when it explains 'Each time you have a failed ATP system, you are back into degraded mode, where you have to depend on the human behavior, and as we have seen so often, the real problem is not so much equipment issues, but what happens when that equipment fails' [2, p.155].

Degraded Modes and Risk Management

Risk assessments help to justify transitions between the different states that have been identified in Figure 1. For example, abnormal or increased loadings can be tolerated for short periods providing that the potential hazards have been identified and appropriate mitigations have been introduced. Similarly, changes in otherwise normal operations can be approved by regulatory authorities providing that the extent and likelihood of negative outcomes have been considered. **There is a danger that organizations will use risk assessments to explain why otherwise 'degraded modes' might be considered as 'normal' operations.** This is particularly apparent when considering the failure of automated systems. For example, the claim that AWS had no implications for safety was rooted in the belief that operations could continue even when it was not available. Hence there would be no additional risks associated with running services where this application was isolated.

It can be argued that all three of our case studies were the result of inadequate risk assessment by the operating and infrastructure companies that were involved in these accidents. Degraded modes eroded the safety margins that usually protected normal operating practices. For example, the Glenbrook report argued that a Rail Safety

Inspectorate should be introduced to ensure that all of the parties involved in running the railways cooperated in their hazard assessments and in their risk mitigation strategies. The justification for the creation of such a body was based on the observation that many organisations seem to be 'struggling' with the prerequisites for safe operations. Some groups used Australian Standard 4292 to guide their risk management while others adopted a combination of this standard and 4360. In some cases, the decision to use both 4292 and 4360 'produced little more than a bureaucratic structure' [2, p.169]. These structures were said to have achieved little in terms of safety outcomes for both staff and the general public.

The Southall accident report also refers to inadequate risk assessments. As mentioned, there was no systematic attempt to assess the likelihood or potential consequences of changes in the priority of different traffic movements across the regional network. The lack of any sustained risk assessment was criticized following the accident because the signaler's decisions routed the freight train in front of the High Speed Train. It is open to debate whether or not a more formal risk assessment would have had any significant impact upon the course of the incident. In particular, those risk assessments that were carried out seem to have had little impact on other aspects of the collision. For example, changes in the staffing at the Old Oak Common Maintenance Depot reduced levels of support for the engineers trying to trace the cause of the reported AWS failure. These changes in demarcation were subject to internal and external risk assessments. However, neither investigation identified the potential stresses that were placed on shift supervisors who struggled to oversee these maintenance tasks [3, p.64]. Similarly, the train operator commissioned a risk assessment before privatization to consider the potential impact of single driver operations. The report was centered on a risk matrix and concluded that for speeds above 110 miles per hour, a second driver marginally *increased* the risk with or without ATP [3, p.59]. However, this report did not consider the risks of single driver operations for High Speed Trains without either AWT or ATP! The investigation into the Southall accident explicitly questioned the role of risk assessment in the regulation of the rail industry. It concluded that 'the situation has been reached where any change not accompanied by risk assessment is greeted with surprise, if not disbelief' [3, p.194]. As we have seen, there are no guarantees that such techniques will anticipate all of the potential hazards that can arise during the operation of safety critical systems. This can, in turn, create overly optimistic results from quantitative assessments. The Inquiry also questioned the varying quality of the processes that were used to assess the risks of railway operations.

Conclusions

Several recent rail accidents in the USA, UK and Australia have raised questions about the relationships between normal and 'degraded modes of operation'. There is often a culture of 'making do' where managers and employees try their best to maintain services. However, these adaptations and 'work-arounds' undermine safety. This paper has begun to identify the reasons why teams of co-workers continue to operate safety critical systems when key elements of their infrastructure have been compromised, for example during routine maintenance. The extent to which workers will adapt to degraded modes illustrates the flexibility and resilience of socio-technical systems. However, we have also identified the dangers that arise for instance when operational staff fail to communicate their concerns about component failures through supervisors to more senior levels of management. In particular, it is critical to ensure that fault reporting systems initiate repairs before 'degraded modes' turn into emergency situations. It must also be possible for operational and maintenance staff to delay operations if they have the well justified belief that safety has been compromised.

We have also identified the ways in which technical changes, such as the introduction of automated warning and protection systems, create particular vulnerabilities for degraded modes of operation. The Southall accident illustrates what can happen when regulations are unclear about the status of these systems. They may initially be considered as aids that are not essential for 'normal' operations. Over time however, AWS and ATP applications are used in a routine manner that creates complex dependencies between the driver and the equipment that they operate. On the one hand, operators can become habituated to cancelling the warnings so that the majority of Signals Passed at Danger occurs even when AWS is operational. On the other hand, the loss of these systems can remove key barriers that prevent accidents or incidents from occurring.

Changes in environmental and transportation policy are helping to increase the role of rail transportation in national and international infrastructure planning. In order to meet projected increases in demand we must continue to rely on the integration of leading-edge technology with legacy systems. In such circumstances, safety must be

maintained in the face of the component failures that characterise degraded modes of operation. The challenges that this creates can be illustrated by the Glenbrook accident report. At the time of the accident, train movements in the CityRail area were managed from a control centre at the Sydney terminal. Different tracks were operated from their own rooms; each one was equipped with very different levels of technological support. Some provided computer-based monitoring while others relied on the pencil and paper based plotting that was used for the West control area involved in Glenbrook. The investigation argued that these different operations should be combined within a single modern control room. Objections that this would create a single point of failure were addressed by arguments that multiple redundant systems could be put in place to increase resilience to degraded modes of operation and thereby maintain levels of service. The accident report maintained that 'a risk assessment done prior to the design stage would no doubt lead to the identification of appropriate controls for any such potential hazard' [2, p.148].

The closing sections have raised a number of caveats about the utility of such risk assessments. These techniques provide high-level means of quantifying the likelihood and consequences of adverse events. Unfortunately, the integrated nature of modern railway operations, the blend of leading-edge and legacy systems, the scale of interacting components all make it difficult to successfully apply existing risk assessment techniques. It is essential that we acknowledge these concerns. Risk assessment techniques cannot, typically, predict all of the ways in which complex rail systems will fail. There is also a danger that risk assessments will be abused to provide a form of post hoc normalization. In other words, these studies are used to reclassify situations as 'normal' when they might formerly have been characterized as 'abnormal' or 'degraded'.

Acknowledgements

The authors would like to thank Richard Popplestone and Graham Lewis of ESR Technology who provided invaluable technical input on the degraded mode operations within the rail industry.

References

1. Railway Group Standards, Section 6, Railway Safety: Operations, February 2007.

2. Special Commission of Inquiry into the Glenbrook Rail Accident-Final Report, Chaired by P. A. McInerney, Special Commission of Inquiry into the Glenbrook Rail Accident, Currently available from the New South Wales Independent Transport Safety and Reliability Regulator, Sydney, Australia, April 2001.

3. The Southall Rail Accident Inquiry Report, Prof. J. Uff, UK Health and Safety Executive Books, London, 2000. ISBN 0 7176 1757 2

4. The Derailment of NorthEast Illisnois Regional Commuter Railroad Train 519 in Chicago, Illisnois, October 12, 2003. US National Transportation Safety Board, Railroad Accident Report, NTSB/RAR-05/03. Ref PB2005-916303, notation 7615A. 2005.

5. L. Bainbridge, Ironies of Automation: Increasing levels of automation can increase, rather than decrease, the problems of supporting the human operator. In J. Rasmussen, K. Duncan and J. Leplat, (eds.) *New Technology and Human Error*, Wiley, Chichester, pp. 276-283, 1987.

Biography

Christine Shea, M Ed, PhD, ESR Technology Ltd, Whittle House, Birchwood Park, Warrington, Cheshire, WA3 6FW. E-mail - christine.shea@esrtechnology.com

Christine Shea is a principal consultant in safety and risk management with ESR Technology. Her work involves the management of risk in complex, safety-critical domains including aviation, rail, the petroleum industry and health

care. Her research interests include the management and organisation of work in safety critical domains, safety culture, the development and implementation of incident reporting systems and human error.

Chris.W. Johnson, DPhil, MA, MSc, FBCS, CEng, CITP, Department of Computing Science, University of Glasgow, Glasgow, G12 8RZ, Scotland, UK, telephone +44 (141) 330 6053, facsimile +44 (141) 330 4913, e-mail – Johnson@dcs.gla.ac.uk, web page http://www.dcs.gla.ac.uk/~johnson

Chris Johnson is Professor of Computing Science at the University of Glasgow in Scotland. He heads a small research group devoted to improving the reporting and analysis of incidents and accidents across safety-critical domains ranging from healthcare, to the military to aviation and rail.