The Team-Based Operation of Safety-Critical Programmable Systems in US Commercial Aviation and the UK Maritime Industries

Chris Johnson,

Dept. of Computing Science, University of Glasgow, Glasgow, G12 9QQ.
Tel.: +44 141 330 6053, Fax: +44 141 330 4913
johnson@dcs.gla.ac.uk

Abstract. This paper analyzes a range of incidents involving team-based interaction with safety-critical programmable systems. The incidents were submitted to NASA's Aviation Safety Reporting System (ASRS) and to the UK Marine Accident Investigation Branch (MAIB) between December 2001 and February 2003. Our results show that incidents, which complicated the team-based operation of safety-critical, computer systems in commercial aviation, are now being reported within the UK maritime industry. This reflects the increasing use of programmable navigation and collision avoidance devices both in ferry operations and in commercial fishing. For example, many incidents in both industries now stem from operators making inappropriate assumptions about the likely behavior of co-workers and their programmable systems even though part of their task is to actively monitor those activities. In the aftermath of adverse events, operators often argue that monitoring was unnecessary because of their previous reliability record. This seems to indicate that greater training is required in order for operators to understand the likely limitations both of their co-workers and the programmable systems that they operate. Our results also show that a growing number of incidents are triggered when teams must rapidly reprogram complex, safety-critical systems in response to unpredictable changes in their operational requirements.

Introduction

The introduction of computer-controlled systems imposes new demands on the operators of safety-critical applications. This has led to novel forms of failure in many different industries. For example, a UK MAIB (2002) report recently described how a fishing vessel deviated from its course and grounded; "the autopilot had developed a fault prior to arriving at the port, and although the skipper had attempted to have it repaired, the fault remained unresolved. He was aware of the wisdom of checking the autopilot against the compass heading, but apparently failed to do so on this occasion. With no obvious indication to remind him that the autopilot was not working, he engaged it with misplaced confidence". Such incidents remind us that the introduction of complex, computer-controlled systems can paradoxically increase the need for team-based interaction. The MAIB argued, "A second person

on watch would have enabled the autopilot malfunction to be identified, and remedial action to be taken. With no redundancy, the skipper was reliant on the correct operation of the navigational equipment and his ability to maintain a proper lookout". Marion Blakey (2002), Chair of the US National Transportation Safety Board, has put forward similar arguments. Speaking in the aftermath of a recent rail collision, she argued that 'this accident could have been prevented with the installation of a backup safety system that would have alerted crewmembers to restrictive signal indicators'.

The importance of team-based interaction for the operation of safety-critical systems has led to the development of training techniques such as Crew and Bridge Resource Management (Sexton et al, 2000). These provide guidance on how to coordinate teams of co-workers during adverse events. They also include training in more routine team-based operating procedures, including the call back of commands. CRM and BRM are widely perceived to have averted many potential accidents. For instance, the US Aviation Safety Reporting System (ASRS) provides the following example of 'Great CRM and Piloting' in which the crew faced an extreme combination of failures; "…the Captain's autopilot dropped off with several warning flags on his flight instruments. He transferred control of the aircraft to me. During descent, various warning lights illuminated, which were reset several times. We ended up with one pitch trim working. The Captain was surrounded by inop flags on his instrument panel, so was unsure of which instruments were still operating. Random electrical warnings erroneously indicated that the aircraft was simultaneously on the ground and in the air… The SO found a second fire extinguisher and discharged it into the continuing red glow in the circuit breaker panel. During the approach, we encountered... failure of both direct lift control auto spoilers. At touchdown, spoilers were manually extended. I selected reverse thrust, but no thrust reversers worked. On taxi in, all three engines were in flight idle. At the gate...the aircraft was still pressurized–Flight Attendants could not open the door. The SO tried to shut down all packs and engine bleeds, but could not. The Captain attempted to shut down the engines with fuel and ignition switches, but engines kept running. Engine fire [fuel shutoff] handles were pulled, and engines shut down. The door was opened from the outside, and the passengers exited" (ASRS, 1999). Reporting systems such as NASA's ASRS provide important insights into the successful team-based interventions that avoid potential incidents. In the following incident, computer-related warning systems and the vigilance of the crew resolve a potentially dangerous situation created by Air Traffic control. A commercial aircraft taxied to the approach end of the runway. The Captain then noticed an aircraft on TCAS, which appeared to be landing. The First Officer confirmed the pilot's observation; "When the TCAS was indicating 700 and 500 [feet] for the aircraft on Final, I asked the First Officer if the aircraft was landing. He stated that it was still landing. I initiated a turn off the runway and advised the Tower that we were clearing the runway. Tower asked if we needed assistance. I stated, '[No. I just didn't want to sit on the runway with that aircraft on short final'. As I turned the aircraft around towards the runway, the other aircraft, a Learjet, landed on the runway exactly where we had been in position" (ASRS, 2002c).

To summarize, the team-based operation of safety-critical computer systems provides a barrier against individual human error. Co-workers can monitor and intervene to support interaction between colleagues and increasingly complex systems. However, team-based operation also creates opportunities for different forms of 'error'. Colleagues may rely on their colleagues to correct their mistakes; co-workers can introduce distractions and can exacerbate the effects of individual 'errors' (Sasou and Reason, 1999, Sexton, Thomas and Helmreich, 2000). This paper differs from previous work in this area because it focuses on team-based interaction with programmable systems. Rather than focusing on the validation of human factors models of decision-making, this paper also focuses more directly on adverse events in two different industries over the last fifteen months.

Incident reports provide insights into adverse events and near misses. They reflect lower severity mishaps than those normally documented in more formal accident reports. They, therefore, provide glimpses of the failures that characterize everyday interaction with safety-critical computer systems. Incident reports also describe near misses. They, therefore, provide insights into team-based interaction as a barrier to more serious failures.

This study looks at two very different domains. US commercial aviation represents a high-technology industry characterized by a relatively small number of large companies. In contrast, the UK maritime industry has a far larger proportion of owner-operators. These industries also differ in terms of the computational technologies that they rely upon. Computer-based control and navigation systems are part of the fabric of US commercial aviation. In contrast, many fishing vessels are just beginning to incorporate computer-based control systems. Ferry operations exploit these programmable devices in greater numbers. In both cases, there is arguably a greater degree of redundancy and a larger margin for error than is the case in US commercial aviation. As we shall see, however, there are strong similarities between the incidents that complicate the team-based operation of safety-critical, programmable systems across these different domains.

Team Weaknesses with Safety-Critical, Programmable Systems

Many incidents in US commercial aviation and the UK maritime industry reveal the limitations of team-based problem-solving (Johnson, 2003). For instance, the second officer of a roll-on roll-off passenger vessel recently attempted to close the vessel's bow doors prior to leaving Calais. He experienced a series of problems in operating the automated control system and called for assistance from the chief and third engineers. He also requested help from an electrical officer. They eventually abandoned the automated system and attempted to close the visor manually using instructions displayed next to the control station. The starboard visor ram and support arm began to buckle and the operation was stopped immediately. An investigation revealed that the starboard support arm-locking bolt was still in the engaged position. None of the team had noticed a light on the control panel indication, which indicated

that the doors were still secured. As a result, two additional control system-indicating lights were fitted to show the position of the locking bolts and modifications were made to the operational instructions (MAIB, 2001). This incident illustrates the importance of good interface design for team-based interaction with complex, programmable systems. The ergonomics of control panel design can prevent operators from observing important warnings when colleagues obscure their view. This incident also illustrates the importance of incident reports in identifying the limitations of team-based problem solving. Groups can compound adverse events as well as resolve them. Rather than explore the reasons why the Second Officer could not complete the operation using the automated system, the group started to manually close the visor even though it was still secured in the open position. A number of researchers have attempted to explain such team-based behavior. Green, Muir, James, Gradwell and Green (1999) describe how "many pilots like to be thought of as fairly bold individuals, and combining a set of such individuals into a crew can make for an unduly bold outcome". This 'risky shift' represents a form of polarization in which groups of individuals whose members are predisposed to accept or to reject a risk will have their predispositions reinforced by being members of that group. Gaba (1994) observes "conflicts between surgeons and anesthetists can result in pressures on anesthetists to proceed with anesthesia even when they believe it is unsafe to do so". He goes on to describe situations in which team-pressures have led anesthetists to misinterpret or even ignore critical indications from patient monitoring systems. Conversely, others have sought to stress the positive role that team-based decision making has upon the operation of safety-critical systems. Bowers, Bickensderfer and Morgan (1998) argue that there is no legacy of 'rugged individuals' within air traffic management and so "there may be no need for awareness-phase seminars or other interventions designed to improve negative attitudes''. They stress the ability of Air Traffic Control teams to construct shared mental models both of the computer systems that they operate and of the intentions of their colleagues.

In order to understand the dual nature of teamwork in both promoting safety and introducing new hazards, it is important to summarize the key factors that distinguish group performance from individual human factors. Tjosvold (1989) observes that as groups grow member, participation declines. He also argues that conflicts increase and co-operation decreases in larger groups. This reduction in co-operation can partly be explained by 'social loafing'. Some individuals contribute less to a group than when they are individually accountable (Latane et al, 1979). Further problems can explain team-based 'errors' with complex, programmable systems. As we shall see, other people can distract operators from safety-critical tasks. Diverting attention away from a task can also make operators worried about performing poorly with the result that they become anxious. A number of problems affect the practical application of these theoretical studies. There is considerable disagreement about the factors that affect group-based performance. The problems of 'social loafing' must be contrasted with Zajonc's (1965) 'drive theory'. He argues that the presence of others can improve performance. Seta, Seta and Hundt (2001) observe that this improvement increases if co-workers are slightly superior to the person operating the system and may also be affected by the degree of group cohesion.

The Flight Deck Gradient

These theoretical disagreements are mirrored by the problems that arise in interpreting incident reports involving team-based interaction. For example, the 'flight deck gradient' often refers to the difference in authority or status that can exist between the Captain and First Officer in commercial aviation. Seta et al would argue that this slight difference in authority might promote rather than inhibit group interaction. However, it can be difficult to find unambiguous evidence for such theories in the documents that are collected by both confidential and anonymous reporting systems. For example, the following report describes flight-crew interaction with a Visual Approach Slope Indicator (VASI); "(The Captain) is an experienced pilot, capable and in no way overbearing…The aircraft begins to descend below the VASI indications, giving finally four reds…I presume the descent *(below the correct glide-path)* is intentional …I inform the Captain we are floating. He seems surprised by my call, but removed power and lands. However, we are between 1/3 to 1/2 of the way down the runway. The Captain appears transfixed by the runway and hasn't engaged reversers as per SOP. I call for reversers and query the autobrake setting of level three out of five available levels. He makes no response. I state that I am increasing autobrake to level four. He doesn't acknowledge. With hindsight I allowed my attitude of respect and friendliness toward the Captain to influence my actions. I was insufficiently assertive once the incident was in progress and prior to the incident I presumed rather than checked the reasons for his flight profile" (CHIRP, 1998). This incident would seem to contradict Seta et al's observation that operator performance improves when higher status colleagues monitor an individual's performance. The pilot reports that he felt inhibited from questioning the actions of a respected co-worker. However, the pilot did eventually intervene. It can, therefore, also be argued that flight crew interaction prevented the incident from having worse consequences. In this interpretation the incident vindicates team-based decision making rather than pointing to a problem with the flight deck 'gradient' (Johnson, 2003).

Misplaced Trust

Team-based interaction often relies upon a form of skepticism about the ability of co-workers to perform necessary tasks. This alienation helps to ensure that operators check and re-check critical commands during the operation of safety-critical systems. For example, the crew of a B737-800 was informed that Air Traffic Control (ATC) training was being conducted in their sector. The plane leveled off at 2,500 feet, following ATC instructions. The Captain was then instructed to turn right onto a heading of 080 degrees. This would have directed them towards terrain rising over 7,500 feet in approximately 2 miles. The crew refused to turn. ATC again replied, "Right turn 080 degrees." The crew stated that they were "unable to comply due to rising terrain to our right and in front of us". They started to turn left in order to clear

the terrain. ATC then asked if the plane was level at 3,500 feet. The crew replied that they were at 2,500 feet. This was the level that ATC had initial assigned them to. Shortly afterwards the left turn initiated by the crew brought them into sight of the airport. They were then cleared for a visual approach (ASRS, 2002a). This incident illustrates how the team-based operation of safety-critical systems often paradoxically depends upon the crews' refusal to comply or cooperate with the instructions of their colleagues. If they had done as they were requested then the safety of the flight would have been placed in jeopardy.

It can also seem paradoxical that distrust is a necessary prerequisite for crew-based interaction with complex systems. However, complacency and a failure to monitor computer-related systems are two of the most common features of team-related incidents in both US commercial aviation and the UK maritime industries. For instance, a recent ASRS report described how a pilot failed to check their First Officer's programming of the Flight Management Computer (FMC). This led to a departure from ATC instructions: "It wasn't until (ATC) informed us, that we realized we were off course ...and it took us a couple of minutes to figure out what had happened. ATC vectored us back onto the departure and gave us a climb clearance. ATC also pointed out traffic, but we never saw it. We are not sure if our error caused, or would have caused, a conflict. The First Officer programmed the FMC. I checked the Route Page to see if it matched our clearance, and it did. It showed the correct departure and transition. I did not check the Legs Pages to see if all the fixes were there. I will next time! I do not know how the two fixes got dropped, but they did, and as a result we got off course... We made an error programming the FMC, then became complacent… This is how we got off course... I should have done a more complete check of the First Officer's programming" (ARS, 200A). Such incidents also illustrate how team-based interaction often creates an illusion of redundancy in the operation of complex, computer-controlled systems. The reporter argues that although they verified their colleague's input, they did not perform sufficiently detailed checks to prevent the incident from occurring.

Similar incidents can be found in Maritime reports. For instance, the UK MAIB describe the grounding of a container ship even though she followed the same route every week. The vessel also had three qualified deck officers in addition to the master and was equipped with a full range of navigational equipment, including two radars and a Global Positioning System (GPS). Visibility was good and it was a clear dark night. The second officer relieved the third officer at midnight and the ship's position, derived from the GPS, was being plotted on the chart from time to time. The charts in use had the courses to steer marked in black ink and could not be erased. An Assistant Bosun shared the bridge watch. Course was altered at 0025, and again at 0047, with the ship's position being plotted on the chart each time she settled on to a new course. At 0243 she altered course again, to 237° and, once again, the position was plotted. About 45 minutes later, the ship grounded at full speed. The MAIB argued that this incident occurred to a well-equipped vessel with fully qualified officers who were familiar with the passage and had no problems in establishing the ship's position in good visibility. However, the ship was on a regular route, and the courses had been indelibly marked on the chart. The numerals 237 were clearly

evident, as was the reciprocal 157 for the return voyage. After the grounding it was found that the automatic steering had been set to 257°. The investigators argued that the officer of the watch had inadvertently set the wrong course, having mixed up 237 with 157 (MAIB, 2001c). In this case, team members failed to detect a transposition error in the programming of the automated steering system. In the previous incident, the Captain failed to detect the First Officer's omission of two fixes in the Flight Management Computer. In spite of the obvious differences between aviation and maritime industries, there are striking similarities between these adverse events.

Erroneous Inferences About Co-worker Intentions

In the aviation domain, programmable systems can be so complex that incident reporting agencies often comment on the 'unusual' or 'extraordinary' performance of the crew in diagnosing the cause of an adverse event. This is illustrated by a recent report submitted by the Captain of a Boeing 737-300. The following report also describes a similar transposition error to the previous example involving the automated marine steering system. This emphasizes further similarities between aviation and maritime incidents in the team-based operation of programmable systems; "We were at Flight Level 250 when Center cleared us to cross 30 miles west of ABC VOR (very high frequency omni directional range transmission navigational beacon). at 17,000 feet. The First Officer was flying on autopilot and dialed in 17,000 feet in the altitude alerter then started programming the Flight Management Computer (FMC) for the crossing restriction. I dialed in ABC on my VOR. Realizing that we were fairly close to the idle power descent profile, I mentioned this and selected Level Change. There was no intersection for the crossing point so the First Officer had to build it, which takes time. When the FMC finished thinking, it indicated that we were well below profile, so the First Officer hit VNAV (vertical navigation system) which brought the descent back to 1000 fpm. That didn't make sense so I looked at the descent profile, which verified what the First Officer had indicated. My VOR readout and the FMC did not agree, but I did not realize what was wrong at the time. I advised [the First Officer] that we were pretty close to the profile and once again selected Level Change. The First Officer was as confused as I was, but accepted the idle power descent profile... I realized in hindsight that he had no idea what I was basing my concern on. Passing Flight Level 200, I concluded that we would make the restriction based on the VOR information, but that it would be close. I called 10 miles, which probably caused more confusion since the FMC indicated that we were significantly farther away. In deference to me, the First Officer increased the descent speed up to our previously assigned limit speed to hasten the descent... We crossed the restriction point at 17,400 feet... We were very close but not perfect. It took a while, but I finally realized that the First Officer had constructed the crossing waypoint correctly but had inserted it after the next intersection instead of before it. The FMC assumed that we were going to fly to the pre-existing intersection then back to the crossing point, which added a number of flying miles to the crossing point and led to the descent profile being in error. Unfortunately the error was caused by a reliance on modern technology which is wonderful but relies upon correct inputs". After the flight, the

Captain “showed the First Officer how to verify that constructed intersections are inserted correctly”.

This incident illustrates how individuals in a team can be called upon to perform ‘extreme problem solving’ in order to address the potential errors that are made by their colleagues. It also illustrates the manner in which the actions of other groups within the aviation system can impose those burdens upon their co-workers. The reporter argued that the entire incident might have been avoided if Air Traffic Controllers could help modern FMC-equipped aircraft by giving crossing restrictions based on predefined intersections that are likely to already be in the on-board database; “any time you have to construct a crossing point, it takes a lot more time and introduces a significant opportunity for error” (ASRS, 2003a).

Many incidents in both the UK maritime industries and US commercial aviation stem from inappropriate assumptions about the intention and actions of co-workers. These assumptions can persuade operators to disregard the evidence provided by computerized warning systems. For example, a ferry recently touched bottom on departure from a Scottish port. There was clear visibility. The master, chief officer, second officer and a quartermaster manned the bridge. They were all very familiar with navigation in the area. The chief officer monitored the vessel's progress using radar and the electronic chart system. There had been no communication between the master and chief officer about the intentions for the passage out of harbor. The Chief Officer thought the master intended to slow down when a navigation buoy was observed on the starboard bow. The chief officer noticed the vessel was swinging too slowly, and moving south of the safe track. He warned the master on the enclosed bridge wing, who immediately instructed the helmsman to apply more port helm. The order was too late. The MAIB argued that the repetitive nature of ferry work could lead to complacency: “everyone knows exactly what to do and there is no need for anyone to communicate”. The vessel was fitted with modern navigational aids. The chief officer, who had sight of the navigational instruments, was monitoring events. He could not, however, accurately interpret the significance of the information provided by automated warning and navigation systems without knowing the Master’s intentions once the fishing vessels were seen ahead. A deviation was made from the usual departure plan but the chief officer could not monitor the master's intentions because he had not been told what they were (MAIB, 2001b).

Further incidents stem from misplaced trust in the programmable devices that perform functions, which would otherwise have been performed by crewmembers. For instance, a recent MAIB report describes how a crew of three operated a fishing vessel. Two of them were cooking breakfast, cutting up bait, pumping out the bilges and cleaning pump filters while also maintaining the watch. Meanwhile, the skipper was asleep on the deck of the wheelhouse. The vessel’s planned track passed 0.35 miles from a rig. The automated radar alarm system was set to a third of a mile. The vessel’s VHF radio was turned off because the skipper argued there was too much distracting radio traffic. The crew of the rig called for help from a stand-by safety vessel that put alongside the boat. Nobody could be seen on the bridge or on deck even after they sounded their horns. The rig went to ‘abandon platform stations’ as a

precautionary measure. A crewmember from the support vessel boarded the fishing boat and found the skipper asleep in a sleeping bag. When the skipper was awakened he was instructed to slow down and steer way from the platform. He did so but protested about being awakened. He claimed that the situation was under control (MAIB, 2002b). This incident illustrates several important aspects of the interaction between teams of operators and programmable control systems, such as the automated radar warning application. In this case, the skipper assumed that his co-workers would maintain an active watch even though they were engaged in several other tasks. The radar warning system should have been used as a form of safety net or as a final safeguard. However, the group working practices seem to indicate a more routine reliance on this device to prevent the vessel from encroaching upon hazards such as the rig.

Distractions, Plan Revisions and Reprogramming Errors

As mentioned, many incidents involving team-based 'failures' seem to stem from a form of complacency. There is an assumption that colleagues or automated systems will perform complex tasks in a reliable manner. Unfortunately, as we have seen this is not always the case. The failure to adequately monitor colleagues and programmable systems not only stems from complacency. It can also be the result of competing tasks and other distractions that eat into the time crewmembers have available to perform necessary checks. A previous NASA study of 107 ASRS incident reports identified 21 different types of routine tasks that crews neglected while attending to another task (ASRS, 1998). It is difficult to determine how many of these interruptions related to the operation of programmable systems. However, 69% of the neglected tasks involved either the failure to monitor the current status or position of the aircraft, or failure to monitor the actions of the pilot who was flying or taxiing. 90% of the competing activities fell into one of four broad categories: (1) communication (e.g., discussion among crew or radio communication), (2) head-down work (e.g., programming the Flight Management System or reviewing approach plates), (3) searching for traffic, or (4) responding to abnormal situations. In 68 of the 107 incidents, the crews reported being distracted by some form of communication, most commonly discussion between the pilots, or between a pilot and a flight attendant. This paper avoids such statistical analyses because incident reports are inevitably affected by submission bias. It is difficult to know whether the 107 selected incidents were in any way representative of those adverse events that complicate the team-based operation of commercial aviation systems. A number of statistical techniques can be transferred from the field of epidemiology to address these biases. The NASA study did not exploit these techniques and they remain the subject of current research (Johnson, 2003). In contrast, the remainder of this paper relies on a more subjective comparison based on an exhaustive analysis of incidents reported by the ASRS and MAIB over the last fifteen months.

Having raised these caveats it is important to stress that both the NASA study and our analysis identify the importance of distractions as a precursor to adverse events in the team-based interaction with safety-critical programmable systems. This can be

illustrated by a recent incident in which the First Officer was forced to go 'heads down' in order to reprogram the Flight Management System when there was a late change to their departure runway. Late changes involving the reprogramming of on-board systems create acute vulnerabilities. In this instance, the First Officer glanced up to see an aircraft at the arrival end of the runway in position with all its lights on. "I said to the Captain, 'No. No. No. We are on the runway!' We were supposed to have turned... At the same time, ATC advised us that we had crossed an active runway. The Captain then understood his mistake... He had heard, "Taxi to" and saw the aircraft on Runway 12, so he thought he had been cleared to cross Runway 12... He stated that something did not seem right". Another incident report describes a situation in which neither crewmember detected reprogramming errors that were introduced in response to a late change. The initial departure was rushed to make the airline and Air Traffic Control schedule. The initial "Computer flight plan was route ABC. However, ATC clearance was via route D-E-F. Original flight plan should have been crossed out or destroyed, so as not to accidentally revert to [the] planned route. [The] First Officer was very experienced and I had complete trust that he was capable of loading the correct waypoints, but both he and [I] failed to use a visible method of marking the computer flight plan. ...99% of the time, the cleared route is the same as the computer flight plan, but not always, as I found out the hard way. ATC caught my error". The crew attempted to fly the original route even though Air Traffic Control had confirmed with them that they were only authorized the fly the revised route (ASRS, 2002b).

Crew Fatigue Impairs the Operation of Programmable Systems

The previous examples illustrate how relatively complex changes to original plans can induce errors in the programming of automated systems. Incident reports in the maritime industry also reveal problems that stem from more mundane issues including crew fatigue. For example, a vessel recently struck a well-known building in a busy estuary in spite of being equipped with ARPA radar sets and an electronic chart system with GPS overlay. As the Master approached the building, he thought he saw a red light close on the starboard bow. Assuming it was another vessel, he ordered starboard helm. The Filipino second officer confirmed the sighting and when no further lights were seen ahead, the Master ordered hard to port to resume his course. Shortly afterwards, the vessel collided with the building's foundation. The incident investigators argued that the building was conspicuous and the vessel was equipped with advanced navigational aids. They concluded that the crews' 'errors' could only be explained in terms of the fatigue that is created by hours of operation and by disturbed circadian rhythms (MAIB, 2001f). Similar causes were identified for the 'mistake' that led to a fishing vessel running aground off the Shetland Islands. The skipper had not slept for about 23 hours and attempted to alter course of the vessel using a joystick control. He did not follow the correct procedure for changing from automatic to manual steering. As a result, he did not realize the vessel had failed to turn until immediately before it grounded (MAIB, 2002c).

Aviation crew operating schedules have arguably been more extensively studied and controlled than those of their maritime counterparts. Fatigue plays less of a role in team-based failures in this domain. There are further differences. In US commercial aviation, Air Traffic Control often detects errors in the interaction between crews and on-board automated systems. Maritime incidents often have more serious consequences because they lack this additional safety net. For instance, a roll-on, roll-off ferry recently grounded in the UK. At the time of the grounding the master, the chief officer, a seaman lookout and the bosun as helmsman manned her bridge. The weather and visibility were both good, however, the approach was through a very narrow channel between drying sandbanks. The bridge team followed a familiar passage plan, which involved the master conning the vessel from the bridge. The chief officer was operating the engine controls according to the master's instructions while the duty second officer monitored the navigation using radar parallel index techniques. However, on departure from the berth the second officer had duties at a mooring station and no one monitored the radar in his absence. The rival tasks that preoccupied the Second Officer created the precondition for this incident to occur. This combined with a navigational mistake that was triggered by a critical buoy that was not lit (MAIB, 2001d).

Crew Failure to Respond Adequately to the Failure of Programmable Systems

Operators often incorrectly assume that programmable systems and their colleague will perform the tasks to which they have been assigned. Their assumptions are often based upon previous observations about the reliability of their co-workers and the systems that they operate (Johnson, 2003). Previous incidents have shown that fatigue, distraction and a failure to communicate key intentions can undermine the validity of these assumptions. In other situations, equipment failures impose burdens upon operators that prevent them from fulfilling the expectations of their colleagues and co-workers. A control system failure on a Scottish ferry illustrates this point. The vessel had two propulsion units, one forward and the other aft. On the morning of the incident, the forward engine had to be started using jump leads from the aft battery. It had insufficient charge to start using its own batteries. Routine pre-operational checks were carried out but, before the main steering controls were tested, the electrical supply was changed from emergency batteries to main power. Following successful tests, the ferry started work for the day. Just before she arrived back, the motorman was given permission to disconnect the emergency batteries to replace a dead cell with a new one. He did so, but found the connecting bridge for the cell was too short. He went ashore to the nearest garage to get a longer connecting bridge. The other crewman also left the vessel to get stores, while the charge hand remained on board. Shortly afterwards, an alarm showed that electrical power had been lost on the main steering controls. The charge hand cancelled the alarm but was unable to restore power. He changed to emergency power and regained control. Shortly afterwards the alarm sounded for the forward main engine. On this occasion he was unable to cancel it and the stern began to slew to starboard. He attempted to correct the movement by using the aft unit but, once again, the controls failed. He tried to restore both main and emergency power, but neither would engage. Unable to do anything further, he

allowed the vessel to slew until it settled against the shore. He then called the harbormaster asking him to contact the other two-crew members. The vessel was now at a 90° angle to the slip. The charge hand tried to shut down the forward main engine so that his crew could board over the ramp. The engine failed to respond. With the vessel now moving slowly along a beach, the motorman finally managed to get onboard through the car deck gate. He was assisted by the charge hand, who had left the bridge to help him. Once aboard, the motorman went to the engine room where he found that the emergency battery charger switch had tripped. He reset it and went to the bridge to assist the charge hand (MAIB, 2001e).

This incident again illustrates the dual nature of many incident reports. They provide insights into the problems that can arise when operators fail to intervene successfully in the operation of complex, programmable systems. Equally, they also provide compelling insights into the ways in which team-members respond to initial 'mishaps' and thereby prevent them from developing into more serious accidents. The following report provides a further, more complex example from the aviation domain. Given the increasing introduction of computer-related systems into the maritime industries it may only be a matter of time before the MAIB receive reports of incidents that are similar in complexity to those of the ASRS. A Fokker 70 was descending through 7,000 feet, on radar vectors for a landing when the "on-board computers generated a level III alert, 'Landing gear not down'". They were well above the alert envelope and traveling faster than the maximum speed at which it would have been safe to operate the landing gear. The pilot noticed that the left seat radar altimeter was reading zero feet. The right seat radar altimeter was indicating the correct altitude and so the crew attempted to switch control to the First Officer's side. "As the descent continued, the flight warning computer added the aural warning, 'Too low gear'. About this time we were given a heading to intercept the instrument landing system final while still descending to 3,000 feet... It was at this time the traffic alert and collision avoidance system (TCAS) added, 'Traffic, Traffic!' As I was looking for the traffic I had to compete with a continuous level III alert chime, "Too low gear" aural alert and now the aural TCAS traffic alert. Again, none of these warnings can be silenced. I looked for the traffic... Sure enough, there was a single-engine high wing aircraft in a left climbing turn. I called out "traffic in sight" about the same time the TCAS started calling, "Climb, Climb!" The pilot flying followed the TCAS guidance and we narrowly missed this aircraft. Somewhere in this sequence the landing gear alert ended... I changed to Tower and the rest of the approach and landing was normal". On the one hand, it can be argued that the crew successfully responded in a flexible manner to this equipment failure. Control was transferred immediately after they noticed the radar altimeter failure. They then divided tasks appropriately throughout the rest of the flight. However, this apparently successful intervention was marred by a number of problems. In particular, the crew were troubled in debrief by their communication over the TCAS warning. The First Officer stated that "a couple of things bother me... I communicated to the pilot flying that I had the aircraft in sight. He could have interpreted this to mean there's no immediate conflict... Had he not followed the TCAS guidance, I think we would have hit the other aircraft" (ASRS, 2002).

Conclusions

This paper has analyzed a range of incidents involving team-based interaction with safety-critical programmable systems. The incidents were submitted to NASA's Aviation Safety Reporting System (ASRS) and to the UK Marine Accident Investigation Branch (MAIB) between December 2001 and February 2003. We have identified strong similarities between incidents in the team-based operation of programmable systems in commercial aviation and the maritime industries. Many incidents in both industries now stem from operators making inappropriate assumptions about the likely behavior of co-workers and their programmable systems even though part of their task is to actively monitor those activities. In the aftermath of adverse events, operators often argue that monitoring was unnecessary because of the previous reliability record. This seems to indicate that greater training is required in order for operators to understand the likely limitations both of their co-workers and the programmable systems that they operate. Initiatives to introduce Crew and Bridge Resource Management are a partial panacea (Johnson, 2003). They provide operators with general training on the error-inducing mechanisms that complicate the team-based operation of complex systems. However, our results also indicate a number of specific problems that complicate interaction with computer-related systems. In particular, many incidents are triggered when teams must rapidly reprogram complex, safety-critical systems in response to unpredictable changes in operational requirements. The reprogramming tasks are exacerbated by problems of interface design that permit the easy omission or transposition of necessary steps in a sequence of instructions, including navigational markers. They also stem from inappropriate assumptions by co-workers about the ease of reprogramming complex systems, for instance Air Traffic Control may underestimate the difficult crews experience in constructing crossing points for Flight Management Computers.

This paper has relied upon a qualitative analysis of the incidents that were submitted to the ASRS and the MAIB over the last fifteen months. A number of factors biased our work. In particular, we are dependent upon respondents notifying the relevant authorities that an incident has occurred. This elicitation bias is an inevitable problem in using any form of incident reporting to support the management of safety-critical applications. This issue explains our reluctance to perform any direct statistical analysis of incident frequencies given that it is impossible to estimate the under-reporting of particular forms of adverse event. In particular, it is likely that team-based incidents may not be reported if groups of co-workers feel implicated by the events that they have witnessed (Johnson, 2003). In other projects, we are using ethnographic and observational techniques to identify those healthcare incidents that are never reported through more formal channels (Randell and Johnson, 2002). This work has yielded some surprising results. In particular, we have identified coping strategies that users will exploit in order to 'get the job done'. These coping strategies include the 'hot' rebooting of safety-critical programmable control systems. Further work is needed to determine whether these techniques might yield similar insights within commercial aviation or the maritime industries.

References

ASRS Callback, NASA Ames Research Centre, (1999) No. 239, (2002) No 273, (2002a) No 274, (2002b) No 275, (2002c) No 276, (2003) No281, (2003a) No 280,

ASRS (1998), Cockpit Interruptions and Distractions, Directline Issue 10, NASA Ames Research Centre, http://asrs.arc.nasa.gov./directline_issues/dl10_distract.htm

C.A. Bowers, E.L. Bickensderfer and B.B Morgan (1998), Air Traffic Control Specialist team Coordination. In M.W. Smolensky and E.S. Stein (eds.) Human Factors in Air Traffic Control, 215-236, Academic Press, London.

M. Blakely (2002). Remarks for the Annual Management Conference of the National Railroad Construction and Maintenance Association, National Transportation Safety Board, Miami, Florida, January 12, 2002. http://www.ntsb.gov/speeches/blakey/mcb020112.htm

CHIRP (1998), Feedback No. 46 http://www.chirp.co.uk/air/default.htm

D.M. Gaba (1994) Human Error in Dynamic Medical Domains. In M.S. Bogner (ed.) Human Error in Medicine, 197-224, Lawrence Erlbaum Associates, Hillsdale, NJ, USA.

R.G. Green, H. Muir, M. James, D. Gradwell and R.L. Green (1999) Human Factors for Pilots, Ashgate, Aldershot, U.K.

C.W. Johnson, (2003, in press). Handbook of Incident Reporting, Springer Verlag, London.

B. Latane, K. Williams and S. Harkins (1979) Many Hands Make Light Work: The Causes and Consequences of Social Loafing., Journal of Personality and Social Psychology 37:822-832.

MAIB Safety Digest, UK Department of Transport: (2001)Vol.1, Case2. (2001b) Vol 3, Case 9. (2001c) Vol.3, Case 1. (2001d) Vol. 2, Case 3. (2001e) Vol. 2, Case 11. (2001f) Vol. 1, Case 7. (2002), Vol. 3, Case 19. (2002b), Vol. 1, Case 19. (2002c) Vol 1 , Case 21.

R. Randell and C.W. Johnson (2002), User Adaptation of Medical Devices. In C.W. Johnson (ed.) Proceedings of the 21st European Conference on Human Decision Making and Control, Department of Computing Science, University of Glasgow, Scotland.

K. Sasou and J. Reason (1999) Team Errors: Definition and Taxonomy, Reliability Engineering and System Safety, 65:1-9.

J.J. Seta, C.E. Seta and G.M. Hundt (2001) Exaggerating the Differences Between Relatively Successful and Unsuccessful Groups: Identity Orientation as a Perceptual Lens. Group Dynamics: Theory, Research, and Practice, (5)1:19–32.

J.B. Sexton, E.J. Thomas and R.L. Helmreich (2000) Error, Stress and Teamwork in Medicine and aviation: cross sectional surveys. British Medical Journal (320)7237:745-749.

D. Tjosvold (1989). Interdependence approach to conflict in organizations. In M. A. Rahim (Ed.). Managing Conflict: An Interdisciplinary Approach. 41-50, Praeger, New York.

R.B. Zajonc (1965) Social facilitation. Science, 149, 269-274