Just a bit in a jigsaw puzzle – Systems Dynamics and Safety in Canadian Aviation

Norman MacLeod
Kitty hawk Training Technology
123 Main Street,
Aldwincle,
Kettering
Northamptonshire NN14 3EP UK
n.macleod234@btinternet.com

Introduction

The concept of a 'system' in aviation safety management is widespread and it is now generally accepted that serious adverse events are the product of systems failures as opposed to single point failures associated with individual performance. The Reason Model of accident causation is a staple of CRM courses worldwide. However, the dynamic properties of systems have yet to be fully explored.

This paper recasts aviation as a hierarchical system of production and then explores the dynamics within and between the constituent hierarchical levels. The paper will challenge the concept of safety as being the product of management activity in an organization, instead we propose that safety is an emergent property of a system. Safety is a reflection of the way individuals work in order to achieve production goals. That said, production processes are themselves a manifestation of strategic decision-making and, therefore, safety in systems can only be achieved through an understanding of how these strategic decisions shape workplace behaviour.

An Overview of the Aviation System

Whereas systems have traditionally been modeled in terms of component parts, more recent exponents, such as Rasmussen and Leveson, have tended to minimize the importance of functional components, instead positioning systems as nested layers of decision-making. The characteristics of a system include hierarchy, control, communication and emergence. These concepts will be elaborated here in the context of aviation. First, though, we need to establish aviation as a socio-technical system of production. People, processes and technology combine to effect production. The 'product' of, or output from, aviation is payload.

The first property of a system identified was hierarchy. This concept refers to the fact that decisions are arranged in an order of precedence. Each level of decision-making is related to the function of the particular hierarchical level. Five such levels are proposed in the aviation system:

The Environment
Facilitation
Exploitation
Organization
Production

The concept of the Environment borrows from broader systems thinking in that it reflects all those external factors that influence subordinate levels but are not influenced in return by events at lower levels. A simple example of an environmental factor is the weather. At any time, weather will influence operations but operations do not influence the weather. The economic situation is an environmental factor in that it produces the demand for payload capacity. The environment, in effect, represents the context within which decisions are made.

The level of 'facilitation' includes those strategic organizations that support the production process but are not, themselves, producers.. This level includes aviation authorities and aircraft manufacturers.

The level of 'exploitation' represents those entities created to deliver production capacity: air operators, military squadrons, civil air support units of various descriptions.

The level of 'organization' represents the social configuration of assets required to accomplish work. This is the traditional focus of CRM training. However, where this iteration differs is that it considers the 'crew' to be any agent having a part in the production process at any specific moment. This 'virtual' team includes on-board and off-board participants and recognizes that the constituted workgroup changes through the life cycle of a specific flight.

The level of 'production' represents the action of individuals engaged in productive activity. This is where payload capacity is generated. Historically, this has been the focus of technical training and has become divorced from CRM. However, taking a systems perspective reveals that this division is flawed, as we will see in the next section.

The 5 components in the aviation system are arranged in a hierarchical order of precedence in that levels are subordinate to those above. It is this hierarchical precedence that allows each level to exercise control over those below. Control is exercised primarily through communication. Orders, instructions, regulation, tasking and approvals from superior levels are used to control subordinate levels. The nature of the work at each level confers distinctive properties, which are captured in the concept of 'emergence'. Emergence reflects the fact that behaviours at each level are not necessarily mandated, rather they arise from the way in which each level achieves its goals.

It was said earlier that systems are characterized in terms of decision-making as opposed to structure. In the model outlined here, each level in the hierarchy makes decisions about how processes should be conducted and then grants 'permissions' to subordinate levels. Of course, in the case of the Environment, decisions and permissions are metaphorical but, nonetheless, tangible. Aircraft operating in extreme weather are at risk. Airlines go out of business during downturns in the economy. At the level of Facilitation and Exploitation, decisions are embodied in technology, in the framing of regulations, design of procedures, granting of approvals, allocation of duties. At the level of Organization, decisions are reflected in the construction of plans and the enactment of collaborative tasks. Finally, at the level of Production, decisions are embodied in action. We will now explore the dynamics of the hierarchical systems model through a set of examples drawn from recent Canadian aviation accidents.

Production – Actors Achieving Goals

Production happens in the workspace. The workspace is the notional site where individuals, technology and processes come together to enact goal-directed behaviour.

In a perfect world, individuals initiate, monitor and terminate behavioural sequences that are planned to meet the needs of the task in hand. In reality, individuals have to modify and adapt behavioural routines in order to contend with perturbations in the operational environment, with contingencies and with unexpected events.

Successful functioning at this level is predicated upon operator ‘knowing’, robust processes and optimized technology. We have deliberately distinguished between ‘knowing’ and knowledge. The latter represents an absolute representation of a domain whereas the former represents the mental modeling of a system applied by an operator in order to comprehend events and select appropriate actions in order to maintain control and achieve desired operational goals. The implication is that operators can be working in situations where their understanding of events is imperfect because of an inadequate mental model, because of a failure to recall relevant information from long-term memory or because of a failure to detect or interpret environmental cues. ‘Knowing’, then, is the mental construction held by the operator at a particular time and used to drive performance. Procedures and technology are both artifacts of the process of designing solutions to problems; they are embodied decisions made a higher levels in the hierarchy. As such, they are fallible and have a probability of containing latent errors. At this level, an operator applies mental representations to generate behavioral routines which, then, serve to control technology within a procedural framework. The following incident illustrates production activity.

On 7 June 2006 (Report A06Q0091) a Bell 206 helicopter was damaged on landing near La Tuque, Quebec, after an in-flight engine failure. The flight had started normally and a pre-flight inspection revealed no oil leaks and the oil tank contents were within allowable limits. En route the oil pressure gauge showed fluctuations within limits but with no other abnormal indications. The pilot made a precautionary landing in a marsh. Advice over the phone from a mechanic resulted in a check of the system and an engine run-up. With the engine now running, the pilot decided to reposition the helicopter on a more convenient road approximately 1 km away, which is when 2 engine bearings failed.

The pilot was involved in constructing a solution to a problem. The oil system appeared normal on initial inspection. The fluctuating oil pressure once airborne was indicative of a possible problem. However, the variation was within limits: oil temperature was normal and the chip detector light was off. One possible contrary indication was a large quantity of bluish smoke coming from the exhaust after shut down. During the subsequent engine run, the oil pressure was stable although in the lower limits of the gauge range and the bluish smoke was still coming from the exhaust. The pilot was faced with 3 options: ignore the symptoms and continue, land now or land at some point before the planned destination. In order to select between these options he had to reconcile the conflicting signals presented to him. Processing information required him to develop an opinion about the state of the aircraft using information presented through his instruments, to incorporate other information known to him and to act within procedural guidelines. However, sensors and gauges, as mentioned earlier, are themselves the result of decisions made at the aircraft design stage. In this case, the oil temperature sensor is located at the oil tank outlet and it is possible for the temperature to indicate normal even when the level is low. However, the values for oil temperature and pressure both contribute to problem assessment. The design of the oil system allows corroborating evidence to be masked from the pilot. There was one piece of important information available to the pilot and that was the presence of bluish smoke, initially on first shut down and then continuously during the engine run and final flight. In fact, the aircraft had issued smoke once before but the problem was eradicated by changing the make of engine oil. In this case, information is mediated through past experience and its meaning modified. The checklist contained 2 advisory statements: where a value for oil pressure or temperature exceeds a limiting value then the pilot must land as soon as possible. However, a non-standard value still within limits requires the pilot to land as soon as is practical. Both statements allow the pilot to exercise discretion. Given the initial unfavourable landing site – a mosquito-infested marsh with difficult access from the nearby road – the pilot used his discretion in order to reposition to a more favourable location.

In this example the pilot was engaged in sense-making behaviour in real-time in order to develop aircraft control strategies. Pilots also engage in planning behaviour in order to minimise workload once airborne. Planning is characterised by information gathering and part-processing of the flight task. Outputs from planning include verification of the legality of the task, aircraft performance parameters, draft contingency plans. Although highly procedural, planning also accommodates discretionary behaviour. On 19 Jan 05 a King Air 200 encountered icing conditions that exceeded the aircraft's systems' ability to cope. The aircraft was unable to maintain altitude and descended below a safe level. The report (A05P0018) noted that, although the pilot inspected the TAFs, METARs and SIGMETs, he did not review the graphical area forecast which called for moderate icing from the freezing level up to 16,000 feet for approximately two thirds of the planned route. This failing was cited as a cause of the incident in the report. The reasons for not checking the graphical forecast were not cited. Data gathering, of which inspecting weather information sources is an example, is a search strategy involving trade-offs between the effort required to inspect data sources and the incremental added value of the data obtained. In this case we can hypothesise that the pilot expected no additional information from the graphical area forecast that he had not already obtained from the sources he did check.

This particular instance throws light on the paradoxical nature of operator production activity in the workspace. The King Air is not approved to operate in severe icing conditions *or other conditions that exceed the capabilities of the aircraft's ice protection equipment* (our italics). The graphical forecast referred to moderate icing and so it is debatable if the pilot would have changed his plan if he had gathered the additional information. Given that forecasts are exactly that – forecasts – they contain an element of unreliability. The requirement to avoid *'conditions that exceed the capabilities of the aircraft's ice protection equipment'* calls for an ability to predict the weather to a degree that exceeds the ability of even professional forecasters.

The estimated flight time was 1 hour 30 minutes and the aircraft was able to cope with the encountered icing for about 40 minutes until the rate of accumulation increased. At that point, the aircraft was unable to maintain speed or climb, 2 strategies that can alleviate ice formation. Management of icing requires judgement to be exercised in relation to the rate of change of environmental factors. Unfortunately, the point at which a problem is recognised is often after the point at which effective action can be taken. The procedural framework for managing icing is, actually, ineffective. We will return to this point later in the discussion of the 'facilitation' level in the hierarchy.

In this section we have outlined the nature of pilot performance in the sense of private, internalised mental activity directed at performing behavioural routines.

These routines allow the pilot to achieve operational goals. Pilot performance is shaped by an understanding of the situation and enacted within a framework bounded by technology and processes. We have chosen a single pilot example to highlight the fact that all performance starts with an individual making sense of a situation and, then, taking action. These actions represent the point at which performance enters the social domain of organized activity.

Organization – Distributed Task Accomplishment

CRM has traditionally focussed on interaction between crew members. Although the boundaries of the crew have been extended to include flight deck and cabin, and passing reference is often made to other off-board agencies, the CRM concept has yet to offer a coherent model of social activity in aviation. The 'organization' level in the systems model recognizes the collaborative nature of aviation. It positions a flight as a task that follows a trajectory from initiation to dispersal. The composition and boundaries of the team responsible for the task at any point on its trajectory are fluid and porous. Thus, on 21 Jan 06 a Cessna 208 Caravan crashed while attempting a forced landing after an engine failure (report A06P0010). Although VMC at the time of the failure, the pilot would have to enter IMC in order to attempt a landing. He sought guidance from ATC with regards to high ground between his current location and his nearest suitable airport. In this instance the task of making a safe landing was shared between 2 elements of the collaborative group – the pilot and ATC.

This collaborative nature of aviation is made clear in the following event (report A04P0397). On 29 Oct 04 a BN Islander nearly collided with a DHC-8 on take off from Vancouver International Airport. The Islander was at Taxiway A, at the threshold to Runway 08R on the north side of the runway. The DHC-8 was positioned on Taxiway L2, to the south and further along the runaway. It was still dark at the time of the event. The Ground controller issued the taxi instructions for the Dash 8 crew and then completed the flight progress strip. The design of the strip is such that space for information is limited and the information about the cleared taxiway – L2 in this case – was obscured. The Ground controller passed the flight progress strip to the Tower controller who was sitting beside him.

The Tower controller cleared the Islander to line up, asking the crew to move forward to allow the Dash 8 to line up behind it. The Tower controller clearly assumed that the 2 aircraft were on the same taxiway and there were several aircraft waiting for take-off at the time. The crew of the Dash was then cleared to line up. They could not see the Islander nor, given their angle of approach to the runway could, they see the threshold area. Because it was still dark, the Islander could not see the Dash 8.

Controllers are required to name the intersection in the take-off clearance if it differs from the threshold but pilots are not required to repeat the intersection in the read-back. The Tower controller had missed the information on the flight progress strip about the Dash 8's actual position. Vancouver has Area Surface Detection Equipment installed but issues of reliability and dependability rendered it useful as an aid only. The Dash 8 was shown as a target on the ASDE at the L2 position but was disregarded as a spurious return by the Tower controller despite the fact that the return moved after the Dash 8 was cleared on to the runway.

As the Islander started its take-off roll, the Dash 8 was moving towards the runway, the crew looking to their left for the Islander they were supposed to be following. At the last moment, the decided to check the up-wind area only to see the landing lights of the Islander coming towards them. They stopped the aircraft and turned on all external lights as the Islander lifted off in front of them.

This example demonstrates how the aviation task is distributed across multiple actors. Historically, CRM has tended to focus on the immediate team who work largely through face-to-face contact. In fact, effective working at the organization level in the system requires skills of collaboration. These include behaviours necessary to establish the bigger picture, negotiation of agreed solutions, verification of responsibilities and monitoring. Traditional concepts of group organization such as roles and responsibilities, status and authority continue to apply but now have to be extended to the distributed, virtual team.

Exploitation – The 'Business' End

Commercial organizations operate at the level of 'Exploitation'. Here, assets are organized in order to support production activities. Airlines do not produce: crews produce. However, airlines configure assets in order to allow production to take place. The mechanics of production are neatly illustrated in an event that occurred on 1 Dec 04 (report A04Q0188). A Beech B300 Super King Air was seriously damaged after it ran off the edge of the runway at Saint-George, Quebec. The case is of interest because the operator was a private company and the company also operated the airfield on behalf of the local community. As such, the entire operation sits outside of the normal regulatory framework. The aircraft, with a crew of 2 and 1 passenger, made an attempt to land off its first approach, flew a non-compliant go-around, and then flew an unstable second approach. Descending below minima, and in reduced visibility, the aircraft touched down on a part-cleared, snow-covered runway. Although the whole approach was questionable, in this section we will look at the way in which the company was configured to oversee operations.

The role of the company is to provision for, organize and control operations. This includes, among other things, acquiring aircraft that meet airworthiness requirements and are appropriate for the task, providing crews that meet licensing requirements, arrange infrastructure to support operations, overseeing operations, managing contingencies, sampling performance to verify compliance and quality standards. In this case, the operator existed to transport company executives, shareholders and their families. Saint-George is the company HQ. The airfield is uncontrolled and is not owned by Transport Canada. Day-to-day operations are overseen by an air transport coordinator who acts as an airport manager, dispatcher, radio operator and also provides a limited weather service (runway condition, altimeter setting, wind direction and speed). The single runway, 06/24, has published approach charts.

Three aspects of the accident throw light on the mechanics of 'exploitation'. The aircraft had departed at 0935 and was expected back at around 1100. Snow began to fall after the flight left. The company had a contract for snow clearance and the runway had been ploughed once already that day. It was agreed that the runway would be ploughed again before the accident flight's planned return time. Runway clearance typically takes 45 minutes and so the air transport coordinator had an expectation that the plough would return at 1000. In fact, the driver did not start work until 1110, barely 15 minutes before the aircraft arrived over the threshold. The first approach, flown by the FO, was unstabilized but, in any case, the Captain called for a go-around as the snowplough might still be on the runway. Radio communications between the coordinator and the plough driver were intermittent because the positioning of the antenna on the vehicle did not allow for continuous line-of-sight. Therefore, full control of the vehicle at such a critical time was impossible. In this first example, the ability to maintain a useable runway was compromised by inadequate equipment and management of assets.

The approach charts for the airfield include a minimum visual range. However, because the airfield lacks approved meteorological observation facilities, these minimum ranges are advisory only. The actual visibility at the time of the second approach was _ mile as opposed to the 1_ miles recommended. The company had not established a mechanism for ground personnel to estimate visual ranges on the airfield. This second example illustrates how organizations are often required to develop ad hoc processes to support operations in the absence of other, more formal, provision.

The final example concerns qualification of crew. A third party provider delivered the company's training using generic, as opposed to company-specific, procedures. The operator had requested specific additional training modules, CRM and CFIT being 2 examples, which were recorded in the operator's training records but were not recorded as actually being delivered by the provider. The company's responsibility to ensure that staff was 'fit-for-purpose' was not met.

Organizations exercise control through various mechanisms, the most widespread in aviation being SOPs. Although the company had SOPs covering the conduct of approaches, the crew's actions were significantly outside of expectations. At this point we start to stray into lower order processes. This simple example illustrates some of the processes required at the company, or 'exploitation', level in our hierarchical system.

Facilitation – Establishing the Aviation Framework

At this level in the system agents are responsible for the strategic decision-making. Regulatory authorities embody decisions in regulations and approval processes. Manufacturers embody decisions in technology and operating procedures. Processes at the strategic level are illustrated in the following report. The fatal accident involved a Cessna 208 Caravan that crashed on 17 January 2004 after take-off from Pelee Island Airport, Ontario, Canada (report A04H0001). On board were the pilot, his girlfriend, 8 men and 2 dogs. All were killed. The aircraft had landed after a short 15-minute flight from Windsor, Ontario. It had picked up some icing in flight and people on the ground commented on this to the pilot. After a short turn-round the aircraft made ready to depart. By now freezing rain was falling. The girlfriend had not been approved to fly as a jump seat passenger and no passenger manifest was produced. Contrary to regulations, the dogs were not carried in cages but roamed freely on the floor of the aircraft. The passengers, a hunting party, were not weighed before departure. The aircraft was considerably overweight, already carrying a burden of ice and exposed to the icing conditions prevailing at the time, when the pilot took off. Observers noticed that the aircraft took most of the runway to get airborne. Shortly after take-off the noise of a crash was heard.

We can identify some environmental factors in this scenario. Pelee Island is the southern-most community in Ontario and, as such, benefits from a government policy relating to transport links to remote communities. Located at the western end of Lake Erie, the island is connected by ferry services to both Canada and the United States. The Owen Sound Transportation Company (OSTC) provides the main ferry service to the island. Once privately owned, OSTC is now a subsidiary of the Province of Ontario government. In winter, once Lake Erie freezes, communication links are maintained by a charter air service. Georgian Express was contracted to provide the service for the 2003-2004 winter.

Transport Canada's (TC) Commercial and Business Aviation Division (CBAD) is responsible for the oversight of commercial air operations that fall within its remit. When an operator applies for an approval to conduct a service, the CBAD is required to assess the safety and viability of the application. The functions of the CBAD are divided between Certification – which deals with new applications and changes to existing operations – and Operations, who deal with the on-going oversight of Air Operator Certificate (AOC) holders, of which Georgian Express was one. In order to fulfil this obligation, the Operations sub-division appointed a Principal Operations Inspector (POI) to work with Georgian Express. The OSTC notified the CBAD of its intention to start the winter air service and was told, in a letter dated 11 December 2003, copied to the Certification subdivision, that the responsibility for an AOC rested with Georgian Express. As the OSTC did not hold an AOC in its own right, the Operations subdivision of the CBAD was not copied in on the correspondence. The air link was conducted as a scheduled service under a subsidy arrangement and, as such, constituted a charter operation and therefore did not require Georgian Express to apply for an amendment to its AOC.

The TC POI has a responsibility to conduct regular inspections and audits of air operators. A scheduled audit of Georgian Express had been started on 11 September 2001 and immediately suspended given the events of that day. The audit was rescheduled for September 2004, based on the POI's on-going assessment of the nature of Georgian Express' operations. However, special purpose inspections can be triggered by significant changes to a company's operations. The commencement of the Pelee flights would be just such a significant change but, as we have just seen, the service was deemed to be a charter, despite being conducted as a scheduled service, and communications concerning the flights had not been copied to the Operations sub-division. The responsible POI did not know that Georgian Express had started operating to Pelee Island.

The design of an aircraft is required to satisfy international standards of airworthiness. The characteristics of the aircraft under different conditions of flight are tested and engineers are required to provide solutions to a variety of safety contingencies. The aircraft cannot be used until it receives a certificate from the airworthiness division of the appropriate authority, in this case the US Federal Aviation Authority (FAA). The effect of ice on aircraft performance is well-known and the regulatory authorities and the manufacturer, Cessna in this case, publish specific regulations, general guidance and seasonal reminders about flying in icing conditions. Of relevance to the Pelee Island accident, there are regulations that relate to the removal of ice, particularly on the wings of aircraft, before take-off and also to take-off in conditions of freezing precipitation. The Cessna 208 Caravan is also fitted with devices to prevent the formation of ice on exposed surfaces critical to flight and to remove ice once it has started to form. Of significance here is that the aircraft design, and its subsequent approval for use, is predicated on operations being conducted within a specific range of conditions. This range of conditions, the associated protection devices, the airworthiness approval and the supporting advice and guidance are manifestations of the decision-making process undertaken when the aircraft was designed. For reasons we will discuss later, it is possible to attempt operations outside of the prescribed scope, as in the case of Pelee Island. At this point, the system is prone to failure.

Of course, there are other actors in this tragedy. As no de-icing was available at Pelee Island Airport, the company provided 2-gallon containers of de-icing fluid with an attached spray for use at remote locations (behaviour at the level of Exploitation). According to procedures, a company flight plan was used to document the flight. The flight plan was used to record details of load, fuel, passengers and aircraft weight and balance. Passenger weights were calculated using a set of industry standard figures ('Facilitation' behaviour). A copy of the completed flight plan was supposed to be left with the passenger agent before departure (Exploitation again). No flight plan was found for the accident flight, nor were any de-icing fluid containers found in the wreckage (behaviour at the level of 'Production').

The accident at Pelee Island illustrates how the conduct of operations at lower levels in the hierarchy occur within a bounded space, the extent of which is notionally limited by the actions of strategic decision-makers. However, as we will see in the next section, the behaviour of the system is often at odds with its intentions,

Dynamics of Systems

Two properties of the system model described earlier are Control and Communication. Control is a property of position in the hierarchy. So, regulators exercise control over operators. Operators exercise control over crews. Within a crew, control is exercised through the social processes of status, authority and role.

Control is typically exercised through communication processes (e.g. rules and regulations), through punishments (e.g. fines) and through denial of permission to operate (e.g. refusal, restriction or removal of AOC privileges). Control is also exercised by constraints on freedom of action (e.g. aircraft must be operated within the design envelope). Communication within systems takes 2 forms: mandated action and design output. Mandated action includes all formal communication intended to direct or constrain behaviour. This includes procedures as well as regulations and is typically contained in manuals, orders, instructions and procedures. Design output is communication about the status of a component of the system and is usually contained in signs, symbols or discrete data outputs. Both forms of communication are intended to direct the action of lower-order actors in the system.

There is a paradox in aviation system dynamics in that the scope for discretionary behaviour increases as we progress down the hierarchical levels; hierarchical control effects are dissipated. This can be seen clearly in the Pelee Island accident. The company has in place a process for flight planning and management and yet individual pilots were ignoring the procedure. The manufacturer provided advice and the regulator provided instructions about the management of icing and yet the pilot seems to have acted outside of the mandated process. The direct exercise of control is difficult in a hierarchical system like aviation because of the delegated nature of work. Individuals act at a distance from central control and are able to exercise discretion in order to achieve operational goals. In fact, actions as defined in procedures cannot be entirely prescriptive in that the system must be able to tolerate and accommodate the normal perturbations encountered in daily operations. Furthermore, communication processes lack effective feedback mechanisms. Communication is typically downward, reflecting the exercise of control. Successful performance is implied by a lack of negative reports in the system. Attempts have been made to increase the upward flow of information, the latest being the routine analysis of digital flight recorder data and initiatives to audit normal operations. Finally, we have issues of ambiguity and the La Tuque helicopter incident illustrates this point well. Both the meaning and the intent of a communication can sometimes be uncertain. This then leads to idiosyncratic or erroneous actions that, in turn, increase the probability of a failure in the system. Control and communication in systems is problematic but these are not the only classes of systems behaviour that can increase risk.

Vaughn, in her book 'Challenger Launch Decision', identified the Normalization of Deviance as a type of behaviour demonstrated at the 'Facilitation' level in a system in which exceptional conditions become normalized in the absence of clear failure. In this case, degradation of protective measures migrated from being a designed barrier to being evidence of designed protection working as planned. In effect, risk was being reset to zero after each launch despite the fact that incremental degradation was being observed. Because the degradation failed to cross a critical threshold the system was deemed to be working 'as planned'. At the threshold between 'exploitation and 'facilitation' we see behaviour that can be called 'Rationalization'. This occurs when apparently rational management leads to unsafe state. A good example is that of maintenance in the DC-9 discussed by Dekker. Over time, harmonization and rationalization of maintenance schedules resulted in the intervals between maintenance events increasing by a factor of 7. Finally, an emergent property of systems is asynchronicity: change made in one area that is not reflected in all other affected areas. Asynchronicity can be formally induced through design or rule changes or it can be manifested in the form of operational 'creep'. In the case of Pelee Island, the operator envisaged the flight to be 2 sectors with appropriate planning and administrative action being done for each sector. Very quickly, pilots began to treat the flight as a single sector with an intermediate stop. This, in turn, resulted in a modified approach to planning. So, the process as planned and envisaged by management (level of exploitation) was modified at the level of production but this changed status was not recognised higher up the system.

One final property of systems we need to address is that of safety. Systems theorists propose that safety is an emergent property rather than an engineered output from systems functioning. In effect, 'safety' is a reflection of the way work is done at the level of production. Attempts to promote safety will only be effective to the degree that they induce a change in behaviour at the lowest level in the system. This is because it is not the system that is 'safe' but, rather, it is the way individuals choose to cat within the system that creates 'safety'.

Lessons from the Systems Perspective

We want to highlight 3 lessons that emerge from a systems perspective: the need to more fully understand how individuals construct solutions to workplace problems; the role of safety management systems; the nature of safety and risk.

We said earlier that work is done at the point of confluence of pilots' 'knowing', procedures and technology. This raises a number of issues. Both procedures and technology have intent; they serve a purpose. A study of annotations made in checklists and manuals found that the 2 most common categories were notes of explanation and notes to elaborate procedures. Pilots seek explanations of intent – the reason why – and more detailed descriptions of method – the 'how' of a procedure (citation). If individuals are to be well-prepared to deal with perturbations and contingencies, then the workplace needs to be fully analysed in terms of possible shortfalls in making sure intent is apparent.

Safety Management Systems (SMS) are now a mandatory requirement. An SMS represents a delegation of authority to conduct oversight. An historical function of the 'facilitation' level has been delegated to the 'organization' level, a reflection of increased resource constraint at the higher level. An SMS is based on hazard identification and a quantification of risk. Hazards are external to the production process and notions of risk attempt to identify a constant that can be applied to processes in order to identify mitigation opportunities. However, in this paper we have attempted to show that production is a fluid and variable activity that responds to changing conditions. A notional 'risk' one day might have a very different value the next. Safety management is unlikely to be effective unless it addresses the nature of the construction of solutions to operational problems.

Finally, and to reinforce the last point, emergence is a characteristic of the systems model and we have attempted to show that safety is an emergent property of the level of production. Risk is resident in the way individuals work. Perhaps it is time to reflect on our current understanding of risk. We need to reconfigure risk as a measure of the gap between the actions required in a situation and the plans executed by agents at the level of production.

Conclusion

This paper has briefly scoped the concept of aviation as a dynamic system, drawing on examples from recent Canadian experience to illustrate key aspects. By recognising the different functions of the distinct layers in the aviation system it is possible to better identify modes of failure and, in term, propose remediation activity. More important, the analysis allows strategic action to be evaluated in terms of effectiveness at the level of production, which is where unsafe behaviour is manifested.

References

Dekker S. (2005). Why we need new accident models. Technical Report 2005-02. Lund University School of Aviation. Sweden

Leveson, N., Daouk, M., Dulac, N. & Marais, K. (2003) A Systems Theoretic Approach to Safety Engineering

Marais, K. Dulac, N. & Leveson, N. (200?). 'Beyond Normal Accidents and High Reliability Organisations: The Need for an Alternative Approach to Safety in Complex Systems'. Paper presented at the Engineering Systems Division Symposium, MIT, Cambridge, MA March 29-31.

Rasmussen, J & Svedung, I. (2000) Proactive Risk Management in a Dynamic Society. Swedish Rescue Services Agency, Karlstad, Sweden.

Wright, P., Pocock, S. and Fields, R.E. (1998). The Prescription and Practice of Work on the Flight Deck