# Understanding the Interaction between Public Policy, Managerial Decision-Making and the Engineering of Critical Infrastructures

**Chris W. Johnson,**
Department of Computing Science, University of Glasgow,
Glasgow, G12 8RZ, Scotland.

+44 141 330 6053
Email: johnson@dcs.gla.ac.uk, http://www.dcs.gla.ac.uk/~johnson

## ABSTRACT
Failures in national and international infrastructures have causes that stretch well beyond the specific events that trigger an accident or incident. The following pages argue that these latent causes can be traced back through the decisions of local management teams to higher-levels of public policy. For example, the 2003 blackout of areas in Canada and the USA was triggered by 'flash overs' that occurred when distribution lines sagged too close to the surrounding vegetation. The causes of this failure can also be traced back to longer term problems in regulating competitive and reliable energy markets. Traders could market electricity without supporting the transmission infrastructure, for example by meeting the costs of vegetation management across thousands of miles of power lines. Similarly the Linate runway incursion was caused when Air Traffic Control Officers (ATCOs) failed to detect that a Cessna had strayed from its authorized taxiways. However, these 'mistakes' were strongly influenced by their technical infrastructure. The lack of effective Ground Movement Radar systems can, in part, be traced back to managerial and regulatory decisions. These, in turn, were influenced by public policy including the joint responsibility for Air Traffic infrastructures within the the Ministero delle Infrastutture e dei Transporti and the Ministero dell'Economia e delle Finanze. Public policy, therefore, creates the context in which infrastructure failures are likely to occur. It is, however, very difficult for engineers to predict the many different ways in which higher level decisions will influence the long-term reliability of critical infrastructures. The following pages, therefore, use an accident investigation technique to provide a detailed graphical overview of the interaction between public policy, local managerial decision making and operator actions. The intention is to alert engineers to the importance of public policy in creating the context in which their systems will be used. We also aim to show politicians and regulators the consequence that their decisions have upon the engineering of safety-critical systems.

*This paper was motivated by observations of a recent workshop on Safeguarding National Infrastructures held in Glasgow, Scotland. It builds on the analysis presented by the other papers in a special edition of Elsevier's Reliability Engineering and Systems Safety journal. These other papers are indicated by references that are not accompanied by a numeric index.*

### Keywords
Critical Infrastructure, Public Policy, Air Traffic Management, Events and Causal Factors charting.

## INTRODUCTION TO THE SPECIAL ISSUE ON CRITICIAL INFRASTRUCTURES
This editorial introduces a special issue on the safety and security of critical infrastructures. It is difficult to underestimate the importance of this topic. There is a rising demand for infrastructure services in many economies. For instance, Licu, Cioran, Hayward and Lowes' contribution to this special edition describe the growth of European air travel. It is predicted that the number of UK air passengers will rise from approximately 180 million in 2005-6 to 475 million by 2030. Most of the expansion has been in scheduled flights within Europe and can be attributed to public policy decisions, in particular, the 1993 European Union directives to open up the internal aviation market. Such increased demand places considerable burdens on the supporting infrastructure, especially regional airports and associated air traffic management services. Newcastle Airport will welcome over 3.5 million passengers between May and October 2006. This represents a 67% rise in passenger numbers since 2000 and an extra 226,600 compared to the previous twelve months [1]. This increased demand has forced rapid changes in the supporting infrastructure. There continues to be a considerable shortage of qualified Air Traffic Control Officers (ATCOs) across most of Europe even though there have been sustained increases in the numbers trained each year. Changes in technology have also been used to increase infrastructure capacity. For example, the increased accuracy of aircraft altitude measurements has made it possible to reduce the vertical separation between aircraft in European airspace. Reduced Vertical Separation Minima (RVSM) has increased capacity by almost 14% following its introduction. However, these innovations cannot sustain longer term increases in demand for infrastructure provision. Additional problems arise for infrastructure provision in the face of rising demand within other areas of the globe. For example, the number of people flying within India each year can be compared to the total number of passengers on the nation's railway network each day. However, this situation is changing. During 2005, there was a 25% increase in passenger traffic. It has been predicted that

the 6-7 million passengers who will use internal air services in India during 2006-7 will increase to over 70 million by the end of this decade [2].

The rising demand for infrastructure resources is not confined to transportation systems. For example, the US Department of Energy has forecasted a 30% increase in energy demand over the next twenty years. In other countries, the need to increase supply is complicated by changes in the public policy of infrastructure provision. For instance, the UK is facing an 'energy gap'; it must replace a large number of coal-fired generators that contravene European directives on emission levels. Although nuclear plants provide a little over 20% of the national generating capacity, the scheduled working lives for most existing reactors will end in 2020. Other countries face different problems as they must develop critical infrastructures to support rapid industrial expansion. During 2003, 23 of China's 31 provinces and major cities had to ration power. This was an increase from only 12 regions in 2002 [3]. The East China Power Grid regularly faces a shortfall of up to 17m kilowatts in the winter months. It seems likely that demand will continue to rise. China currently produces one-thirteenth the amount of electricity per head that the US generates, and one-eighth the amount per person of Japan. In other countries, public policy has been identified as a key inhibitor on necessary infrastructure development. The Confederation of Indian Industries criticized the low and unstable voltages that have forced many companies to install their own generators. The Confederation has called on central government to cut through regional bureaucracy so that the transmission network can allow excess power in one region to be sent to other areas.

The importance of critical infrastructures does not simply stem from the growing demand for service provision. The increasing integration and complexity of many technologies creates a situation where failures in one industry can have knock-on effects across many others. For example, Cowie et al provide a detailed analysis of the impact of the North American and Italian blackouts on computer networks during 2003 [4]; "While the very largest provider networks (the Internet backbones) were apparently unaffected by the blackout, many thousands of significant networks and millions of individual Internet users were offline for hours or days. Banks, investment funds, business services, manufacturers, hospitals, educational institutions, internet service providers, and federal and state government units were among the affected organizations". Patterson and Apostolakis extend this analysis in their contribution to the special edition. They present a method for identifying critical locations that might offer particularly tempting targets for terrorist attacks or areas of particular vulnerability to meteorological events, including floods. Their approach takes into account the convergence of several different infrastructures within these locations.

Other areas of public policy raise concerns over the sustained provision of reliable infrastructures. In particular, the unbundling and deregulation of energy infrastructure in both Europe and North America have created situations where it can be difficult to ensure that the physical transfer of energy follows the associated financial exchanges. It can also be difficult to ensure that the physical and financial exchange mechanisms take into account the capacity of the underlying transmission networks. Similarly, the increasing demand for low cost air transport and the liberalization of air transport operators has increased the pressure on many European governments to support the 'privatization' of air traffic management organizations. Just as in the power industries, this has created particular problems as new infrastructure providers balance the demands of market competition with effective safety management.

A host of other factors combine to focus public and political attention on the engineering of critical infrastructures. The increasing use of synchronized terrorist attacks has revealed the vulnerability of commercial buildings and mass transit systems, for instance in London, Madrid, Mumbai and New York. Bier, Gratz, Haphuriwat, Magua and Wierzbicki's contribution in the special edition provides further examples as they assess the vulnerability of power transmission networks to terrorist 'interdictions'. Counter terrorism agencies have disrupted potential attacks on other infrastructure targets, including nuclear facilities such as Lucas Height outside Sidney. The means available to terrorist groups also increase concern for infrastructure targets. This point is illustrated by the release of Sarin in five carriages on three of Tokyo's ten underground railway lines during 1995. Similarly, Mohamed El Baradei, the UN chief nuclear inspector has warned of a "race against time" to stop a terrorist nuclear outrage. The International Atomic Energy Agency continues to express concern over the trade in radioactive materials. There had been around 630 confirmed incidents of trafficking in nuclear or other radioactive materials since 1993 [5].

The engineering of critical infrastructures is complicated because companies and regulators must consider uncertain threats, such as those posed by terrorist organizations, while also striving to exploit technological innovations in changing markets. These challenges are compounded by immediate meteorological events and longer term climatic changes. Many areas of Europe are facing sustained periods of drought. Others have experienced flooding on an unprecedented scale, some of which seem to be connected to the loss of run-off areas where flood planes and other natural defenses have been lost to urban development. The events surrounding hurricane Katrina demonstrate both the fragility and resilience of regional infrastructures to individual storms. The US National Oceanic and Atmospheric Administration (NOAA) warns that 2006-2007 will also be above 'normal' while 2005-6 witnessed record numbers of major storms in several States. Over the last twelve months, the Gulf of Mexico has experienced 15 hurricanes.

There is considerable controversy over the existence of long and medium-term changes in regional meteorological conditions. It seems clear, however, that even the expected statistical variations in weather patterns are placing heavy burdens on our existing infrastructures. Local economic conditions have fuelled changes in demography that stress regional infrastructures. For example, there are particular problems in ensuring that water supply continues to meet demand in the South East of England and in areas such as Silicon Valley in the USA. The local nature of these problems creates different demands on infrastructure engineers. For example, UK water companies are working to renew a legacy infrastructure given significant losses through leakage and where they only have knowledge about the physical location of Victorian subsystems.

*What is a Critical Infrastructure?*

The previous paragraphs have identified many of the reasons why governments and the general public have begun to focus on the reliability of critical infrastructures. These include the general problem of ensuring that supply continues to meet increasing demands on service provision. They also include the threats created by terrorist actions and by the knock-on consequences that occur when failures in one system are propagated across other infrastructures. The inter-relationships between critical infrastructures also lead to considerable complexity. These factors combine to create new challenges for traditional engineering techniques. We are working in an environment where it may be important for engineers to understand the way in which high-phase angle differences in high-voltage electricity supplies may ultimately lead to the loss of Internet services in countries that are remote from the failure in the service network [4].

These interconnections between many different infrastructure systems make it particularly difficult to derive a precise definition of what is, and what is not, part of a 'critical infrastructure'. The US National Infrastructure Protection Plan (NIPP) provides a framework that is intended to "prevent, deter, neutralize, or mitigate the effects of deliberate efforts by terrorists to destroy, incapacitate, or exploit them; and to strengthen national preparedness, timely response, and rapid recovery in the event of an attack, natural disaster, or other emergency" (page 9) [6]. The national critical infrastructure includes "assets, systems, and networks, whether physical or virtual, so vital to the United States that the incapacity or destruction of such assets, systems, or networks would have a debilitating impact on security, national economic security, public health or safety, or any combination of those matters" (Page 103). This broad definition builds on the concept of critical national infrastructures that was first codified in section 1016(e) of the US Patriot Act of 2001 (42 U.S.C. 5195c(e)). This recognizes that private business, government and the national security apparatus depend on an interdependent network of infrastructures, which include telecommunications, energy, financial services, water, and transportation sectors.

The contributions of Bier et al and of Patterson and Apostolakis illustrate the importance of the 'primary' infrastructures that lie at the heart of the definitions embodied within the Patriot Act. National power transmission networks, water and waste systems are clearly important for public health and economic prosperity. The work of Licu et al illustrates another perspective on primary infrastructures when they consider the safety of air traffic management. We describe these as 'primary' systems because government agencies, typically, consider them to represent the most vulnerable elements in national infrastructures. It is important to stress that these vulnerabilities change over time and that new techniques will be required to safeguard new forms of 'primary infrastructure'. For example, Renaud's paper offers a fresh perspective on authentication as a means of addressing the security of e-commerce. Although this stretches previous definitions of critical infrastructures, this work is important because it illustrates the need to look beyond the traditional focus on energy, waste and water. Balducelli, Bologna, Lavalle and Vicoli reinforce this point as they look at the protection of information intensive critical infrastructures. Their focus on emerging failures follows a growing number of papers looking at unexpected interactions between multiple, concurrent and complex systems [7]. It is also important to consider 'secondary' infrastructures. These are systems that are essential to quality of life and commercial success but which present less obvious targets for terrorist actions. In other words, these systems form a key component of national infrastructures but they extend the scope beyond the particular focus of legislation such as the Patriot Act. For example, Zheng's contribution looks at trade-offs between journey times and the relative safety of routes across local road infrastructures. This work has important consequences as many areas of Western Europe and North America face gridlock and with rapidly increasing levels of car ownership in emerging economies, especially in China.

A common theme amongst all of the papers in this collection is that at some level they all deal with the engineering implications of public policy. This represents an important new focus for work on reliability engineering and system safety because government bodies are often poorly equipped to understand the technical consequences of high-level policy decisions. Public policy, typically, includes a requirement to ensure the reliability of national, critical infrastructures irrespective of whether they support power distribution, water supplies, air or road transport etc. These concerns are not restricted to the mixed economies of Europe and North America. For example, China is assessing the extent to which it should rely on foreign investment as a means of funding infrastructure expansion. The concerns raised about overseas control of key assets within China are very similar in tone to those expressed in the United States when the Chinese petrochemical company CNOOC tried to acquire Unocal. Further problems arise in areas of national infrastructure that have been traditionally looked on as natural monopolies. Most governments refuse to allow multiple commercial service providers within the Air Traffic Management of a single nation state. Similarly, it can be difficult to create market competition over

power distribution when there is only a single physical network of cables and pipes. However, it is important not to assume that government responsibility for infrastructure provision should automatically lead to market intervention. Many countries in Europe and North America are endeavoring to find mechanisms by which commercial organizations can compete within an open market to lower the costs of infrastructure provision. This creates tensions when companies choose to compete on price rather than on the provision of social goods, including reliability and safety. Public policy, therefore, creates the context in which infrastructure failures are likely to occur. It is, however, very difficult for engineers to predict the many different ways in which higher level decisions will influence the long-term reliability of critical infrastructures. The following pages, therefore, use an accident investigation technique to provide a detailed graphical overview of the interaction between public policy, local managerial decision making and operator actions. The intention is to alert engineers to the importance of public policy in creating the context in which their systems will be used. We also aim to show politicians and regulators the consequence that their decisions have upon the engineering of safety-critical systems. The events leading to the Linate runway incursion are used as a case study for this introduction.

## SYNOPSIS OF THE LINATE RUNWAY INCURSION

The Linate accident happened on the 8th October 2001 when a Boeing MD-87 was taking off from runway 36R at Milan's Linate Airport [8]. The MD-87 collided with a Cessna 525-A, which taxied onto the runway. The MD-87 carried two pilots, four attendants and one hundred and four passengers. The Cessna carried two pilots and two passengers. All occupants of the aircraft were killed along with four ground staff who were working in a baggage handling building struck by the MD-87 after the runway collision. The official ANSV report identified the human factors causes that led the Cessna's crew to mistakenly cross the active runway under, low visibility conditions. It also balanced these factors against a number of organizational and technical limitations in the infrastructure systems that supported the airport's operations. This accident had wider repercussions and prompted international initiatives in Europe and the US to reexamine the causes of and barriers against runway incursion. It, therefore, provides an appropriate case study to illustrate the manner in which public policy can help to shape the engineering decisions that may lead to infrastructure failures. In order to illustrate these influences, an accident modeling technique is used to trace back the immediate causes of the collision through a series of infrastructure failures to the managerial and organizational precursors for the runway incursion.

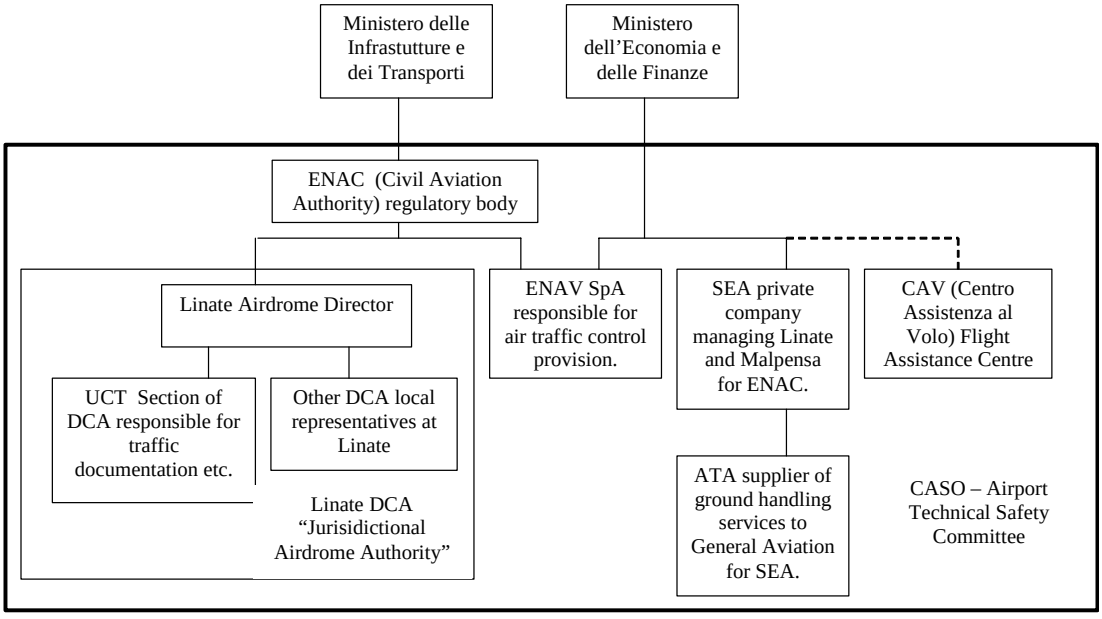


**Figure 1:** Simplified Organizational Structure Prior to the Linate Accident

Public policy is defined to be guidelines or rules that results from the actions of governmental and quasi-governmental organizations. Public concern over infrastructure reliability often persuades government agencies to intervene directly in the engineering of many large scale computer systems. There is considerable controversy over whether such interventions directly contribute to incidents and accidents. It can be argued that governmental intervention is necessary to ensure 'social goods', including reliability, that cannot be guaranteed under free market competition. In contrast, it is also argued that government intervention creates the preconditions for failures when deregulation fails to consider the implications for infrastructure investment. The Linate accident has causes that stretch back into the public policy of Air Traffic Management in Italy. As mentioned in the introduction, many European governments were struggling to resolve the tensions between

market economics and the need to maintain extremely high levels of safety. Figure 1 shows how the operational staff at Linate were also caught between the economic competition and safety regulation. These are represented by the Ministero delle Infrastutture e dei Transporti and the Ministero dell'Economia e delle Finanze. This is a common tension in modern air traffic management as market forces play an increasing role in former state monopolies. Perceived changes in the priorities associated with economic competitiveness and with safety regulation have also been identified as root causes of accidents in a wide range of industries, as diverse as UK railways and US space missions.

The public policy tensions between infrastructure provision and economic competitiveness led to a complex division of responsibilities at Linate. The service provider, ENAV, was controlled by the ministry of finance but operated under 'surveillance' from the ministry of transport. The official investigation concluded that "the management and operational situation at the airport was complicated and involved three major organizations ENAC (Italian Civil Aviation Authority), ENAV (Air Naviagation Service Provider) and SEA (company managing Linate airport for ENAC). No effective performance agreements did exist between involved organizations regarding safety matters" [8]. Figure 1 sets the scene for the Linate accident. The multi-party reporting and management structure led to many organizational difficulties. In particular, the ANSV argued that the divided reporting illustrated in Figure 1 prevented the airport authorities from fully developing appropriate Safety Management Systems.

## Managerial and Organizational Background

The opening sections of this editorial described this common tension in modern air traffic management as market forces play an increasing role in former state monopolies. Perceived changes in the priorities associated with economic competitiveness and with safety regulation have also been identified as root causes of accidents in a wide range of industries, as diverse as UK railways and US space missions. Such tensions are hinted at in the ANSV report but are not made explicit. Figure 2, therefore, uses a simplified form of Events and Causal Factors (ECF) diagram to analyze the background to the Linate runway incursion. This notation was pioneered by the US Department of Energy. We do not claim that this is the only or even the best modeling technique that might have been used to support our analysis [9]. It was selected because it provides a graphical overview of the events leading to accidents and incidents. It is also one of the techniques recommended by organizations, such as NASA, for use in the analysis of aerospace accidents [10]. Ellipses denote contributory factors that combine to make events more likely. Events are denoted by rectangles. This diagram looks at some of the many ways in which the organizational structure directly affected the context in which the accident occurred.

ECF diagrams provide a graphical means of representing and reasoning about the ways in which organization and managerial factors help to create the preconditions for incidents and accidents. These factors combine to create vulnerabilities in the critical infrastructures that are intended to support the operation of safety critical systems, such as Linate air traffic management. Figure 2 records the observation that CASO, the Airport Technical Safety Committee only met sporadically. This is represented by a contributory factor approximately mid-way down the diagram on the left-hand side. One of the factors that led to this was the need to improve the Safety Management Systems in operation at Linate prior to the accident. This apparent shortcoming also partly explains a failure to learn from previous incidents. These are shown as four separate events, including a very similar incident to the collision between the Cessna and the MD-87 which occurred only 24 hours before the accident. In this incident an aircraft taxied along taxiway R5 instead of R6; the Controller was only alerted to the incident when the crew realized their potential mistake.

Figure 2 also illustrates the way in which higher-level public policy priorities interacted with local safety-management practices. The ECF diagram records the ANSV's observation that most of the early concern about runway incursions came from North America rather than Europe. This may partly explain why transatlantic initiatives to address the problem began to make significant progress some three months before the collision leaving insufficient opportunity for many of the subsequent recommendations to be adopted at Linate. These factors combined with the issues that stemmed from the lack of effective Safety Management. Together they contributed to a situation in which there was no effective runway safety plan. The lack of a fully developed runway safety team may also help to explain the absence of runway safety awareness campaigns, of a failure to ensure compliance with International Civil Aviation Organization (ICAO) runway requirements and for well integrated plans to deal with runway emergencies.

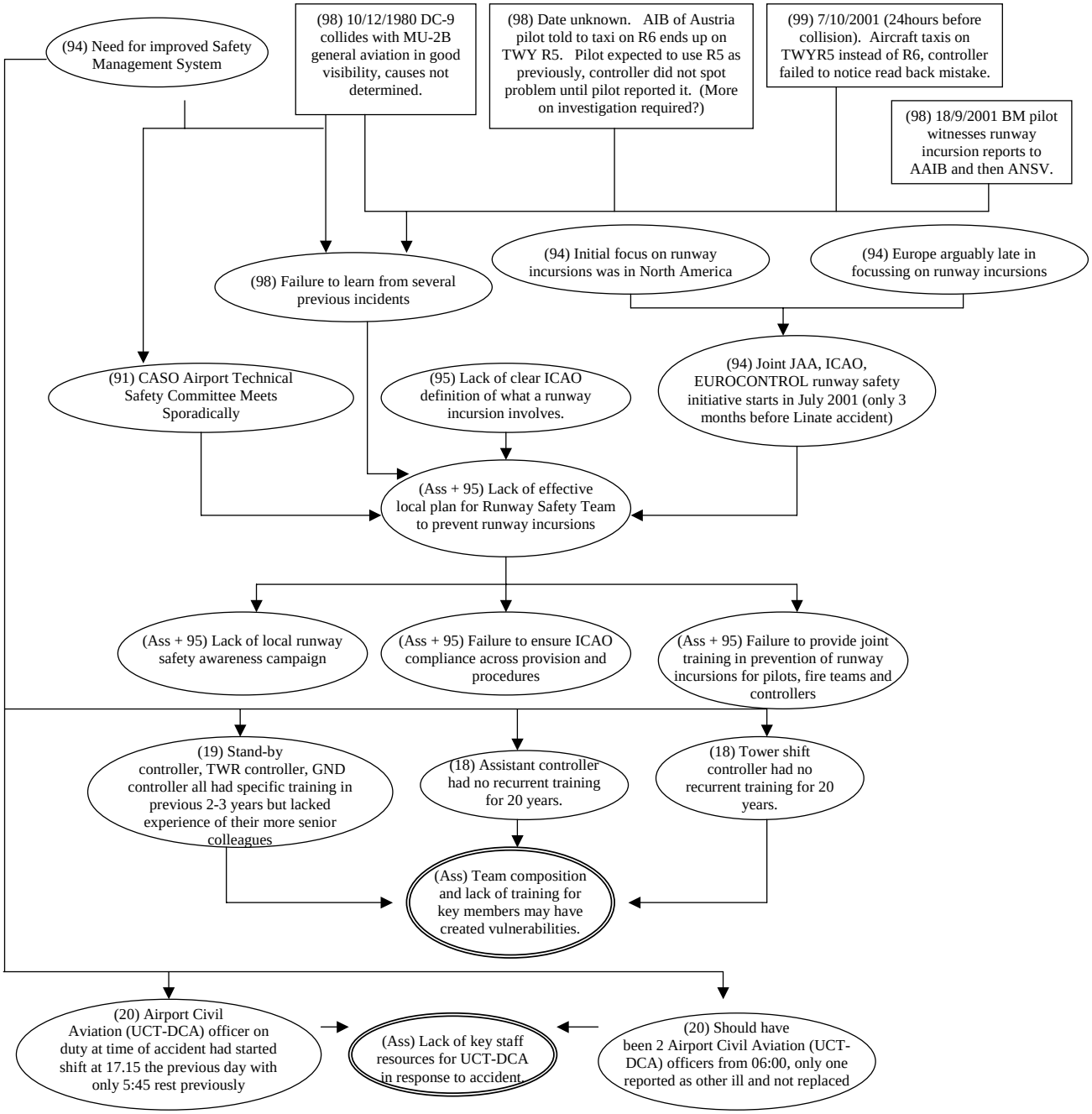


**Figure 2:** Contextual Factors Stemming from Organizational Issues Prior to the Linate Accident

The ECF diagram can be used to trace the consequences of these higher-level issues on the technical and organizational infrastructures immediately before the accident. Figure 2 includes a link between the need to improve Safety Management Systems and the lack of staff in the DCA (Airdrome Judicial Authority) and the UCT (Traffic documentation section). There would usually have been two UCT officers on duty but only one had turned up for duty. Fortunately, their colleague on the previous shift was still present even though they had worked a continuous total of 13 hours on duty. Such "failures to adhere to prescribed obligations" provide specific examples of the ways in which problems in safety management create the vulnerabilities that were exposed during the accident.

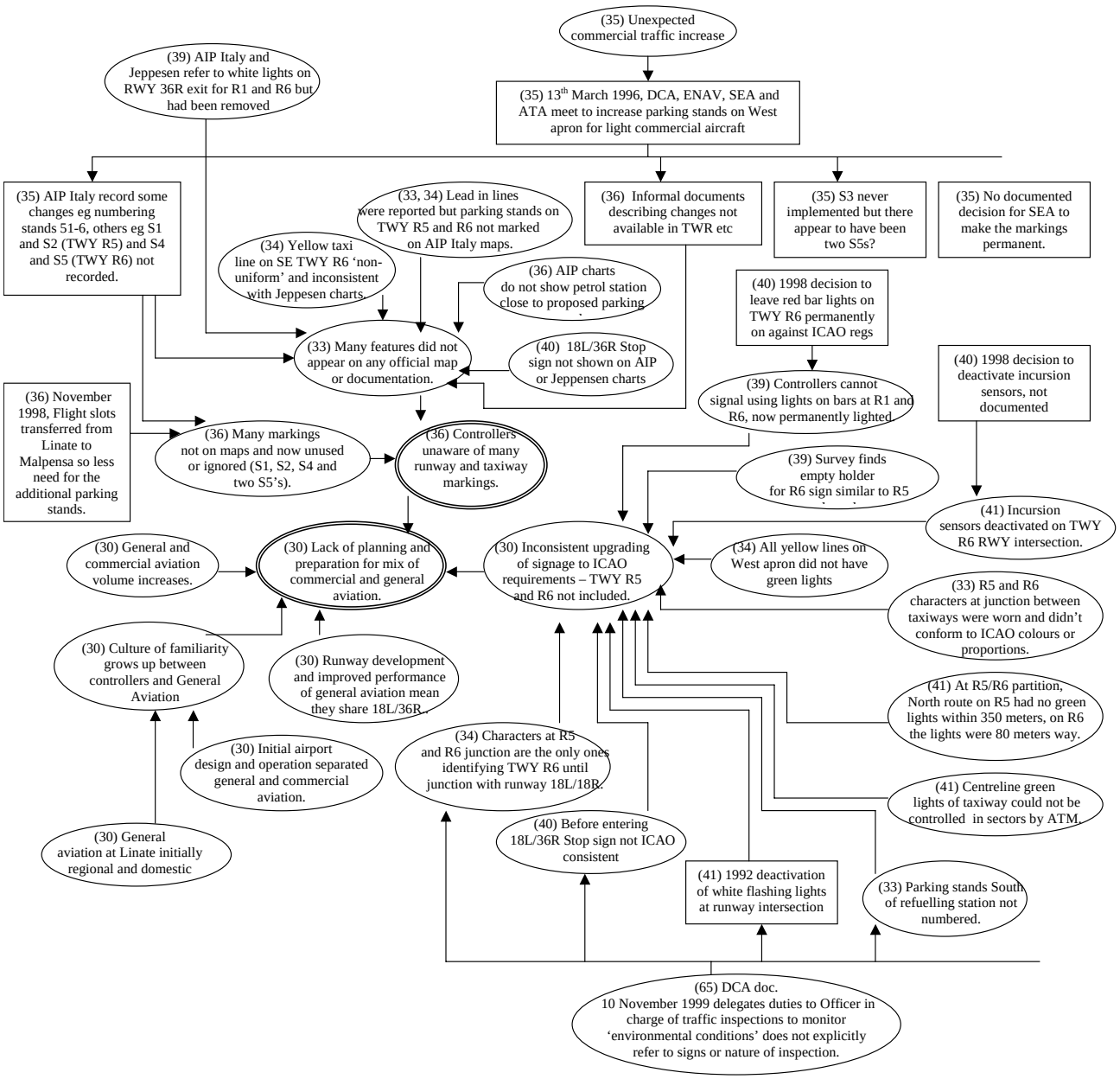


**Figure 3:** ECF Analysis of the Runway Infrastructure at the Linate Accident

### Runway and Taxiway Infrastructures before the Accident

Figure 3 extends the analysis by illustrating the impact that European and national policy had upon the operating infrastructures that contributed to this accident. Previous sections have mentioned that the 1993 European Union directives helped to open up the internal aviation market to increased levels of competition. At Linate, there was a gradual rise in the volume of commercial traffic. One consequence of this was that many of the operational groups, identified in Figure 2, met to consider increasing the parking stands on the West Apron to accommodate more aircraft. These proposals formed part of a number of infrastructure changes that were intended to support the rising levels of demand mentioned in the opening sections of this paper. However, the ANSV report criticized the lack of documentation to support the changes that were proposed by this meeting. There were also inconsistencies in the parking stands that were finally developed. For example, the signs for stand S3 never seems to have been installed and yet there were two areas marked as S5. This created the potential for confusion when crews reported their positions to controllers as they passed S5. These omissions were symptomatic of wider problems in the aerodrome documentation available to aircrews and controllers. For example, the Jeppensen charts of Linate did not show that yellow taxi lines were marked on taxiway R6. The right hand side of Figure 3 also illustrates the consequences of a further change in the operating infrastructure facing ATM personnel before the accident. As can be seen, many of the flight slots at Linate were transferred to Malpensa in November 1998. This transfer meant that there was less need for the additional parking stands at Linate. In consequence, the new bays were largely ignored. These changes combined with the lack of accurate documentation left ATM personnel unaware of many of the

markings that aircrew could see as they moved along the taxiways and onto the runways. These problems contributed to the accident as it became hard for the crew of the Cessna to confirm whether or not they were on the correct taxiway.

Figure 3 not only identifies the impact that rising demand had upon the airport infrastructure, it identifies changes in the mix of commercial and general aviation at Linate. Initially, the design and operation of the airport had separated these different forms of traffic. The general aviation had been largely domestic or regional and the ANSV refer to a 'culture of familiarity' between ATM personnel and the aircrews. However, as we have seen, there had been a gradual increase in traffic at Linate. Runway developments and the increasing power of aircraft used by general aviation pilots created a situation in which runway 18L/36R was shared by an increasingly mixed range of traffic. A further consequence of this was that ATM personnel gradually absorbed the additional overheads associated with synchronizing this mixed-use traffic as they moved from the parking areas, to the taxiways and the runways.

The previous ECF diagram also shows how a DCA document delegated responsibility to the officer in charge of traffic inspections to monitor the 'environmental conditions' associated with the runway and taxiway infrastructure. However, there is no explicit mention of the types of inspections that might be appropriate to meet this objective. Partly in consequence, modifications to the runway and taxiway infrastructure at Linate did not meet ICAO requirements. These included the 1992 deactivation of white flashing lights at the runway intersection and the 1998 decision to deactivate incursion detectors. The former might have warned crews that they were about to enter an active runway while the latter might have helped Air Traffic Control Officers to detect a potential runway incursion. Further problems were created by the lack of control over critical sections of runway and taxiway lighting. ATM personnel could no longer alter the configuration of these light sources to provide positional cues to aircrew, for example by flashing lights on and off in particular areas of the runway. Some of the inconsistencies with ICAO regulations and wider safety provisions stemmed from decisions made many years before the accident. The fact that they had not been addressed after previous incidents arguably reinforces the need for improved Safety Management Systems. It also underlines the need to provide better support for the responsible individuals, such as the 'officer in charge of traffic inspections', and groups, including the 'runway safety teams' anticipated by the working groups on runway incursion [11].

### Technological Infrastructure before the Accident

The Linate Air Traffic Management officers were able to call upon a range of information and control systems. The precise nature and composition of this technological infrastructure was largely determined by the wider economic and public policy context that was mentioned in previous sections. For example, Figure 4 shows that Linate used analogue Aerodrome Surface Movement Indicator (ASMI) radar. Increasing levels of traffic following European liberalization exposed the reliability and low definition of this system to a point at which ATM personnel began to look for an alternative. There was a plan to introduce a NOVA 9000 Surface Movement Guidance and Control System (SMGCS) using video camera technology. The old AMSI system was taken out of service some 3 years before the accident. The plans to install the new system were jeopardized when DGAC, the predecessor of the Italian Civil Aviation Authority (ENAV), objected to the antenna location. They argued that this would involve additional expense by constructing a temporary structure that would then be moved once a new Tower was built. It was also argued that the proposed structure might hinder visibility and that there were few reported problems in handling ground traffic at Linate. The ANSV do not explicitly consider the relevance or strength of this argument given the previous incidents noted in this report. Equally, the DGAC might not have been told about such previous incidents and hence would, from their point of view, have been justified in reaching this conclusion. The ECF diagram in Figure 4 notes this possible objection by showing the 1980 collision between a passenger aircraft and a commercial plane as a counter example. It is possible to draw further links between public policy and vulnerabilities in the technical infrastructure prior to the collision. The ECF diagram in Figure 4 illustrates the DGAC's concern that the new system would not harmonize with other European initiatives. This last point is particularly interesting as a reason to delay expenditure on a significant component of a ground-based safety net. It seems to be counter-intuitive that ATM personnel would be deprived of an important tool so that the eventual system would be consistent with a European initiative that was intended to harmonize safety provision.

The lower portion of Figure 4 uses the ECF formalism to continue the analysis. In July 2000, ENAV assumed many of the previous responsibilities held by DGAC. One side effect of this hand-over was that approval was finally granted for the development of the new Surface Movement Guidance and Control System. The antenna was to be located in the same position as the previous Aerodrome Surface Movement Indicator (ASMI) radar. The ECF diagram also shows that at the time of the collision this upgrade project was further stalled as mothballed hardware had to be re-serviced before the new system could be delivered. As we have seen from Figure 3, the runway incursion sensors had already been deactivated on TWY R6. In consequence, there was "no possibility" to confirm the positions of the various aircraft on the morning of the collision using technical aids.

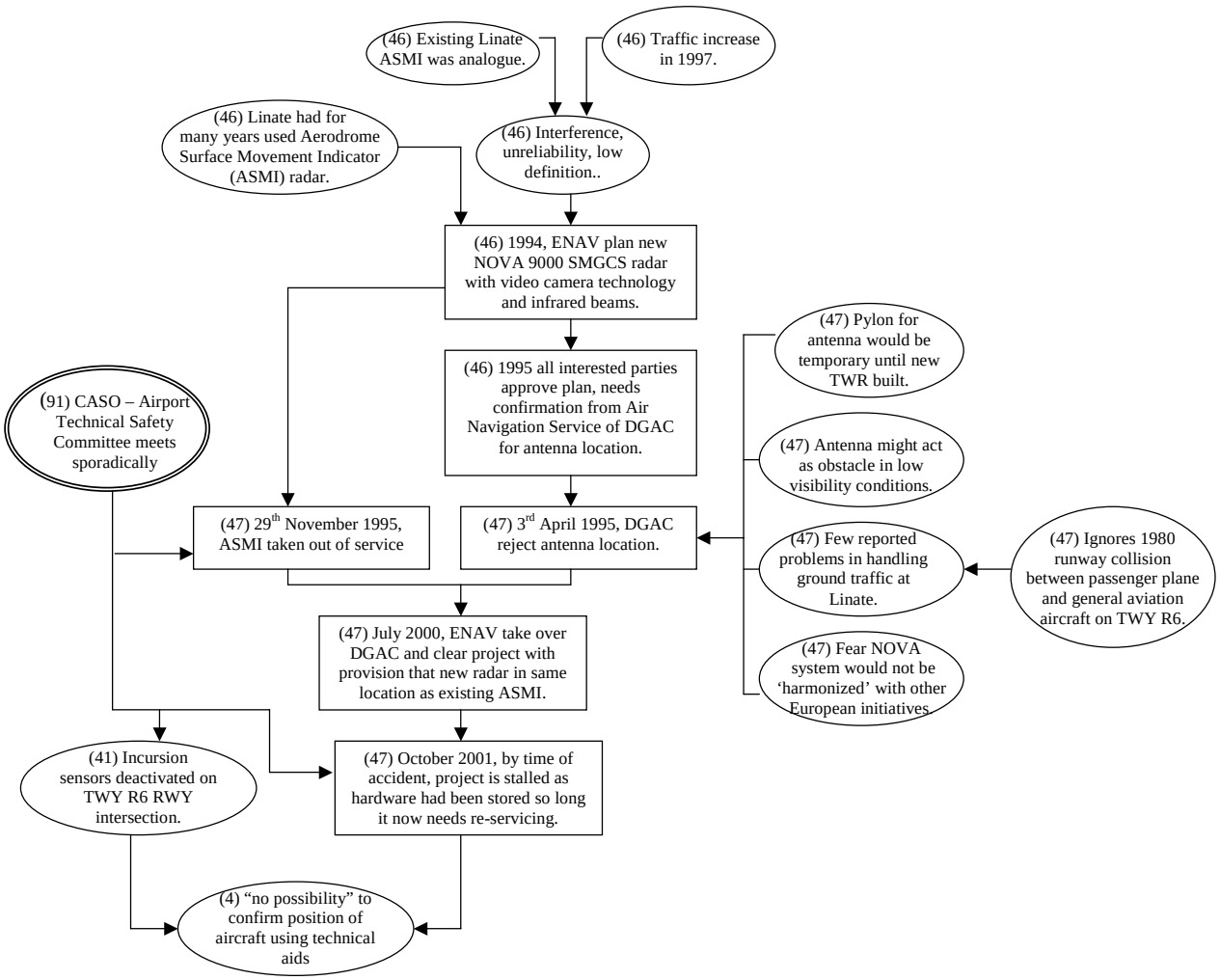


**Figure 4:** ECF Analysis of Technological Infrastructure at the Linate Accident

To summarize, the liberalization of European air traffic had combined with a range of other market forces to increased demand for the provision of air traffic services at Linate. This had exposed the shortcomings of the existing analogue ground movement radar system. However, plans to install a new digital application were delayed both by planning restrictions and by further public policy concerns that any future system should be consistent with wider European standards. In the meantime, the existing system fell into disuse and critical infrastructure was mothballed. This led to further delays when the final investment decisions were made to improve the ground movement radar systems. As can be seen, the previous ECF analysis provides a graphical overview of the many complex ways in which public policy and local decision making combine to create potential vulnerabilities within the legacy systems that support technical infrastructures.

### Immediate Events Leading to the Incursion

Figure 5 uses an ECF diagram to form a bridge between the wider infrastructure issues and the immediate events that led to the accident. It begins with the observation that there was an Automatic Terminal Information System (ATIS) broadcast at 04:50 advising of low visibility. Neither the Cessna nor its pilots were qualified to take-off under the Cat II/III conditions that held on the morning of the accident. It follows that they should not have started the flight. We consider two possible explanations, although there are others. Firstly, the crew may not have checked the ATIS announcements. This is marked as an assumption in the diagram and can only provide a partial explanation. The crews' own assessment of the prevailing meteorological conditions should also have alerted them to the possible dangers. Figure 5 also considers the possibility that they heard the ATIS announcement but failed to act on it, either because of commercial and personal pressures or because the ATIS announcement did not spell out the Cat status of the aerodrome under the prevailing meteorological conditions. It can be argued that ATM personnel should have checked the license conditions of the aircraft to ensure that they were permitted to operate in the low visibility conditions that currently held at Linate. However, ATM staff were working under a relatively heavy loading. In addition, Figure 2 has described how the initial dominance of local and regional general aviation at Linate may have led to the development of a culture of familiarity between ATM personnel and these crews. The reduction in traffic following the movement of slots to Malpensa may also have contributed to working practices that routinely cleared

general aviation operations even though the controller's manual stated that ENAC was responsible for checking aircraft and pilots' clearance for low visibility operations.

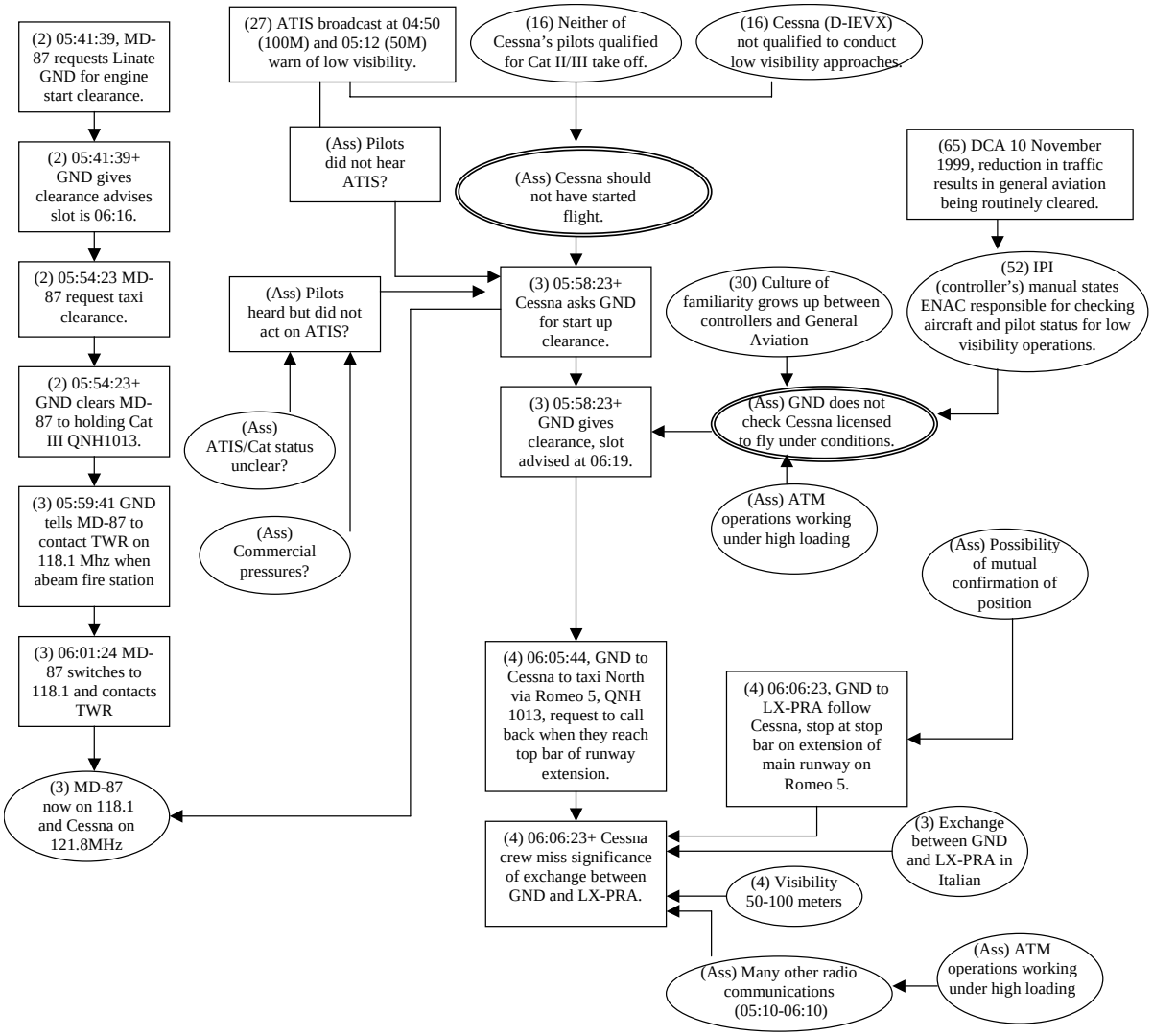


**Figure 5:** ECF Analysis of the Linate Accident – Initial Events on the Morning of the Accident

The left-hand sequence of events in Figure 5 describes how the MD-87 commenced its departure. This included the comment that the aircraft was to taxi to the 'holding position Cat III, QNH 1013". This analysis continues to the point at which the MD-87 transferred their radio frequency to that of the Tower (TWR) while the Cessna continued to communicate with Ground Control (GND) on 121.1MHz. It is important to remember that some nine minutes elapsed between this handover to the TWR and the time of the collision. It might be argued that the protocols used for such handovers should be re-examined given that the opportunity for GND, TWR and the two crews to coordinate their actions was now significantly reduced. The common channel of communication between the GND controllers, the MD-87 and the Cessna diverged into two separate and distinct communications channels between GND and the Cessna and between the TWR and the MD-87 from 06:01:24 onwards. The previous ECF diagram also describes how GND personnel cleared another aircraft LX-PRA to follow the Cessna until the stop bar on the extension of the main runway on taxiway R5. This exchange was in Italian. This may partly explain why neither the crew of the MD-87 nor that of the Cessna was able to use this clearance to identify their relative positions [12]. Equally, the crew of LX-PRA may not have been able to see that the Cessna was no longer in front of them given the reduced visibility on the taxiways.

Figure 6 builds on this analysis and includes the assumption that the Cessna's pilot and co-pilot did not question whether they were on the correct taxiway at this stage because the GND control had given them permission to continue taxiing. The ECF diagram again includes insights from the previous analysis of the environment at Linate. In this case, the crew did not question their position because there were no external prompts to indicate that they might have been on R6 rather than R5. A placard indicating that the crew was on R6 may have been missing. Figure 6 also shows that the Cessna's crew crossed the STOP markings 180 meters before RWY 18L/18R onto TWY R6. The ECF diagram reiterates points from Figure 3 that the STOP sign was not ICAO compliant. The sign was not shown on AIP or Jeppensen charts even though ENAV regulations required that the TWR should stop all aircraft at the signal on TWY R6.

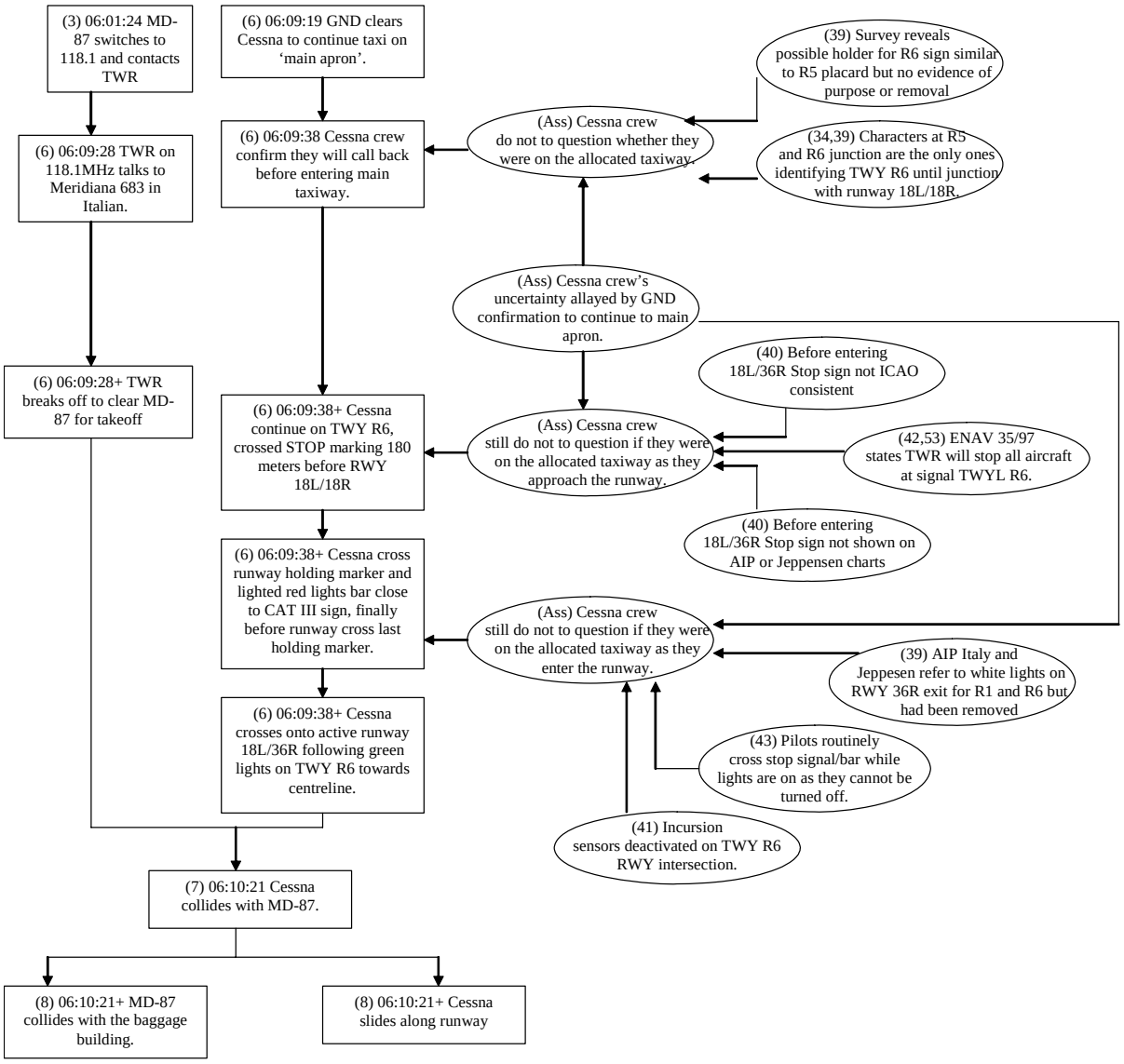


**Figure 6:** ECF Analysis of the Linate Accident – Events Immediately Prior to the Collision

At some time shortly after 06:09:38, the Cessna crossed the runway holding marker. They passed an illuminated red light bar close to a Cat III sign. Again it must be assumed that they were disoriented and did not at this stage question their assumed location on the appropriate taxiway short of the runway. The ANSV provide some information about the reasons why this final set of defenses might have been broached when they argue that pilots routinely had to pass illuminated stop signals because ATM personnel could not routinely turn them off. This diagram also includes further observations on inconsistencies between the signage and official documentation. As before, however, it is uncertain whether there inconsistencies were immediate causes of the accident. There is no evidence that the Cessna crew attempted to use this documentation to trace their position on the taxiway at this relatively late stage in the accident. Their decision to cross onto the active runway may also have been influenced by the path of the green lights on TWY R6 that led onto the centreline of 18L/36R.

### Events Following the Linate Collision

Figure 7 extends our analysis to consider the events that occurred immediately after the two aircraft collided. As can be seen, the MD-87 went on to strike a baggage building that was situated close to the runway. This raises further questions about infrastructure engineering. Although the location of this structure conformed to the relevant DGAC criteria, an ENAV survey had shown that it encroached the permitted area by around 1 meter. Additional lighting had been added to warn crews about the building. This was of little benefit once the two aircraft had collided and the ANSV concluded that the position of the building was 'decisive' in absorbing the violent impact of the aircraft (page 48). Such findings illustrate the

importance of extending any analysis of infrastructure failures beyond the immediate events leading to any particular mishap. In this case, the location of the baggage building may have exacerbated the consequences of the collision. The physical infrastructure did little to mitigate the outcome of the accident.

The previous sections of this paper have argued that public policy decisions combine with local managerial and organizations decisions to create a context in which infrastructure failures are likely to occur. It is important to extend this analysis. Policy decisions and managerial failures do not simply create the vulnerabilities that lead to accidents and incidents. They also contribute to environments where it can be difficult to create effective plans to cope with those failures that do occur. In other words, the same problems that contribute to infrastructure incidents also undermine the resilience that is needed to cope in the aftermath of an adverse event. For instance, the Linate response was hindered by a failure to learn from previous drills that had been organized to prepare for future incidents. These organizational vulnerabilities combined with the adverse meteorological conditions to delay the arrival of emergency services after the collision, illustrates by the ECF diagram in Figure 7.

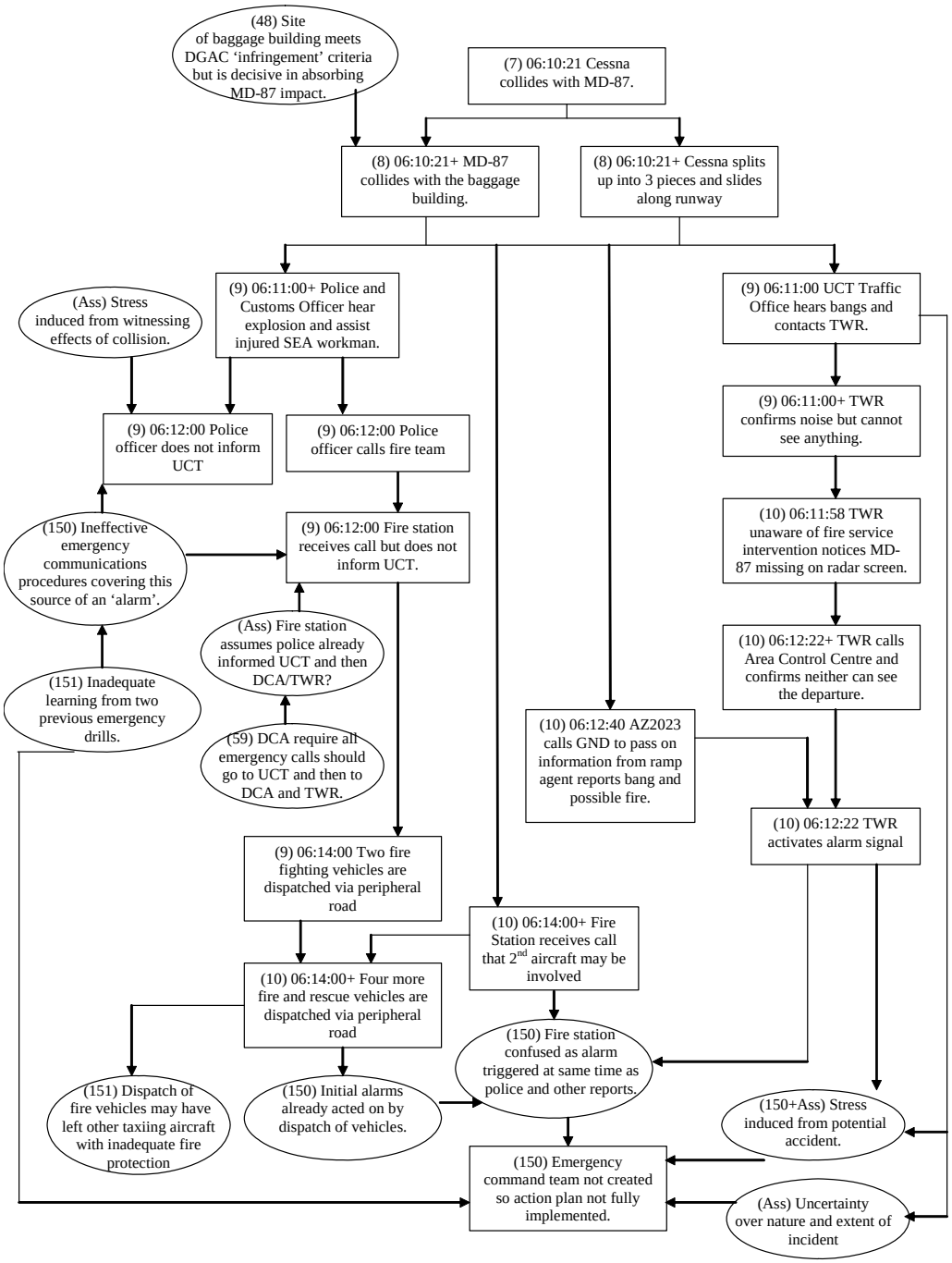


**Figure 7:** ECF Analysis of the Linate Accident – Events Immediately After the Collision

Figure 7 extends the analysis of post accident events to consider communications problems that frustrated attempts to coordinate the response to the collision. A Police Officer who was close to the baggage facility heard the collision and rushed to assist the injured. They then contacted the fire station. However, he did not contact the Traffic Documentation staff (UCT) who should have coordinated the response according to the prearranged emergency plan. One consequence of this was that ATM personnel were not immediately alerted to the initial report. The officer's decision to call the Fire Service is entirely understandable given the stress of witnessing the accident. It can be argued that even if the police officer, acting under the stress of the moment, had failed to contact the UCT to coordinate the response then Fire personnel should have reported to them. However, Figure 7 shows that the Fire Officers may have assumed that the Police had followed the DCA's recommended procedures and had already made this call. This assumption like the others that have been explicitly represented in previous ECF diagrams can be tested against witness statements and evidence not presented in the official report. In contrast, the Fire Officers acted immediately to dispatch two vehicles via a peripheral road without notifying UCT personnel.

The failure of communications between the emergency service and the UTC coordinators may have hindered the establishment of an emergency response team. However, UTC personnel were alerted to the incident even without calls from the Police and Fire Officers. The Traffic Office heard the collision and contacted the TWR. They then attempted to confirm which aircraft were involved. After subsequent calls with the Area Control Centre they realized that the MD-87 was missing. The TWR activated the alarm signal as required by the emergency plan. However, the stress and uncertainty of a potential incident can again be used to explain why neither the ATCO not the UTC staff took the steps necessary to create an Emergency Command Team [13]. This emergency team was supposed to coordinate the response to such incidents. It was also intended to ensure that the pre-arranged emergency plan was fully implemented. A key issue here is that the same lack of coordination that led to the failure to convene the emergency team also prevented the coordinated response that the emergency team was intended to address. This form of vicious circle had not been adequately addressed in the previous drills. This analysis also illustrates a number of further points about the failure of complex infrastructures. Firstly, and most importantly, it is essential that reliability managers and the administrators of public policy take time to study 'real world' incidents so that they get a direct impression of the chaos that can emerge in the aftermath of adverse events. Very often drills simulate 'ideal' situations in the aftermath of infrastructure failures. This not only undermines the credibility of these exercises but it also illustrates a continuing failure to learn the lessons of incident such as the Linate collision. Secondly, the confusion in the aftermath of this collision again illustrates the impossibility of separating the performance of physical and informational infrastructures from the situated, team-based decision making that characterizes emergency response.

The fire station received a second call indicating that two aircraft may have been involved in the incident and, therefore, dispatched four more vehicles. The lack of coordination may have affected this decision as the ANSV argue the dispatch of so many appliances may have left other taxiing aircraft with inadequate fire protection (page 151). This is a significant concern given the uncertainty in the aftermath of the collision and the possibility of wreckage being dispersed across runways and taxiways. In the meantime, the alarm signal from the TWR may have added to the Fire Service confusion. They had already acted on two previous warnings. Hence, it is likely that they concluded they had taken sufficient actions without inquiring about the formation of the command team or explicitly communicating information about their actions back to the TWR. In particular, it seems likely that the Fire Service assumed that TWR personnel already knew the location of the collision. This assumption was unwarranted; ATCOs lacked this vital information as they continued to piece together information about the aircraft that might have been involved in the collision.

## SUMMARY

This paper introduces a special edition of Reliability Engineering and System Safety that is devoted to the development, analysis and operation of 'critical infrastructures'. It is difficult to be precise about what is meant by 'critical infrastructure'; definitions tend to be ambiguous and broad. The US National Infrastructure Protection Plan includes any systems that contribute to "security, national economic security, public health or safety, or any combination of those matters". Some of these systems are familiar, for example Bier et al discuss the reliability of power transmission systems. Licu et al discuss the reliability of Air Traffic management. Zheng's paper considers the reliability of road traffic systems. Other systems play an increasingly important role within the national infrastructure as defined by the US protection plan. Renaud considers the problems of Internet authentication within economic security. Balducelli et al address the way in which information systems form a critical component of traditional power transmission networks. It is also important to stress that there are critical interactions between multiple infrastructures. For example, Patterson and Apostolakis introduce techniques for considering the vulnerabilities that are created by the mesh of power and information systems that underpin most urban conurbations. It is to be expected that these interconnections will increase. In particular, information technology provides the glue that binds physical exchanges to financial transactions across many different infrastructures, including deregulated energy and transport markets.

Rather than simply summarize the content of these different papers, this introduction has argued that the causes of infrastructure failures typically stretch well beyond the specific events that trigger an accident or incident. In particular, we have described the manner in which the Linate runway incursion was caused when Air Traffic Control Officers (ATCOs) failed to detect that a Cessna had strayed from its authorized taxiways. However, these 'mistakes' were strongly influenced by their technical infrastructure. The lack of effective Ground Movement Radar systems can, in part, be traced back to managerial and regulatory decisions. These, in turn, were influenced by public policy including the joint responsibility for Air Traffic infrastructures within the the Ministero delle Infrastutture e dei Transporti and the Ministero dell'Economia e delle Finanze. Unfortunately, it can be very difficult for politicians, civil servants and engineers to predict the many different ways in which higher level decisions will influence the long-term reliability of critical infrastructures. We have, therefore, used Events and Causal Factors (ECF) charts to provide an overview of the Linate accident. The intention has been to extend the usual application of ECF charts in accident investigation to capture the interaction between public policy, local managerial decision making and individual actions. The aim has been to alert engineers to the importance of public policy in creating the context in which their systems will be used. We have also provided politicians and civil servants with an indication of the consequences that their decisions can have upon the safety management and reliability of complex infrastructures.

**Acknowledgements**

I would like to thank Tony Licu and Gilles le Galo for their comments and encouragement with this work and their insights into the Air Traffic Control issues in this incident.

**REFERENCES**

[1] BBC Online, Record Bank Holiday for Airport. London, UK. Last accessed 18th July 2006,

http://news.bbc.co.uk/2/hi/uk_news/england/tyne/5027254.stm

[2] S. Biswas, India Worried Over Air Fare Wars, BBC Online – South Asia. London, UK. Last accessed 18th July 2006,

http://news.bbc.co.uk/2/hi/south_asia/4634091.stm

[3] BBC Online, China warns of more power cuts, Asia-Pacific. London, UK. Last accessed 18th July 2006,

http://news.bbc.co.uk/2/hi/asia-pacific/3715984.stm

[4] J. H. Cowie, A. T. Ogielski, B. J. Premore, E. A. Smith and T. Underwood, Preliminary Report into the Impact of the 2003 Blackouts on Internet Communications, Technical Report, Renesys Corporation, 21st November 2003.

[5] BBC Online, UN Warns Of Nuclear Terror Race. London, UK. Last accessed 18th July 2006,

http://news.bbc.co.uk/2/hi/asia-pacific/3991305.stm

[6] US Department of Homeland Security, National Infrastructure Protection Plan, Washington DC, Last accessed 18th July 2006, http://www.dhs.gov/interweb/assetlibrary/NIPP_Plan.pdf

[7] C.W. Johnson, What are Emergent Properties and How Do They Affect the Engineering of Complex Systems? Reliability Engineering and System Safety, in press, 2006.

[8] Agenzia Nazionale per la Sicurezza del Volo (ANSV), Milano Linate, ground collision between Boeing MD-87, registration SE-DMA and Cessna 525-A, registration D-IEVX, Reference A/1/04, 20th January 2004.

[9] C.W. Johnson, A Handbook of Accident and Incident Reporting, Glasgow University Press, Glasgow, 2003.

[10] NASA, NASA Procedural Requirements for Mishap Reporting, Investigating, and Recordkeeping, NPR: 8621.1A, Code Q/Office of Safety and Mission Assurance, Washington DC. 2004.

[11] J. Rasmussen, Risk Management in a Dynamic Society: A Modeling Problem. *Safety Science* 27:183-213, 1997

[12] E. Hutchins, Cognition in the Wild. Cambridge, MA, MIT Press, 1995.

[13] D. Woods and R. Cook, Perspectives on Human Error: Hindsight Biases and Local Rationality. In R.S. Durso et al., eds., *Handbook of Applied Cognition*. New York: Wiley, pp. 141-171, 1999.