The Implications of September 11th for the Nuclear Industry

John H Large

Large & Associates, Consulting Engineers, London, United Kingdom

After the events of 11th September, it is perhaps just a short and logical step for terrorists to latch onto how highly hazardous plants might be triggered into releasing energy and toxins via an aerial attack. If and when so, could it be that such plants cannot provide a robust defence against aerial attack and are there particularly vulnerable parts of the buildings and processes that, if penetrated, could lead to a devastating release of energy and toxins?

Nuclear plants are such highly hazardous plants. These plants undertake a variety of processes, some of which involve intensely radioactive materials and highly reactive chemicals. Moreover, being nuclear there is a public perception of dread and fear (ie a fate worse than death) associated with radioactive release which might, it could be argued, render plants such as BNFL Sellafield attractive targets to terrorists. However, to mount an attack on a nuclear plant the terrorist cell would have to plan ahead, locate the particularly hazardous plants and stores, determine the amount and nature of the radioactive contents and how readily this might be dispersed into the atmosphere, and identify the most vulnerable aspects of the buildings and containments of the targeted plants.

This paper examines how and by which means those planning such a hypothetical act of terrorism might obtain this sort information and, from this, how potential target systems and processes within a nuclear plant are identified. The work has intentionally confined itself to information and documentation available in the public domain, although it is assumed that those involved would either possess or successfully seek some relatively elementary knowledge of building construction, radioactive materials and substances, reactor fuel, its radioactivity and chemistry.

The outcome is disturbing. First, the requirement that aircraft crash, irrespective of the forecast accident frequency, be accounted for in the regulatory safety case was not introduced until 1979 for nuclear reactors and 1983 for chemical separation and nuclear fuel plants such as those at Sellafield - examples of where the nuclear industry have taken this into account, such as for the Sizewell B PWR, are almost dismissive of the risk solely on the basis that the calculated frequency renders such an accidental event to be entirely incredible and, hence, there may have been little incentive to include for such a remote event in the design. Second, nuclear plants such as Sellafield are almost totally ill-prepared for a terrorist attack from the air – the design and construction of the buildings date from a period of over 50 years, many of the older buildings would just not withstand an aircraft crash and subsequent aviation fuel fire, and some of the buildings, now redundant for the original purpose, have been crudely adapted for storage of large quantities of radioactive materials for which they are clearly unsuited. Third, the design of the most modern plants does not seem to provide that much defence (in terms of containment surety and segregation of hazardous materials) against an aerial attack.

Overall, the nuclear industry defends its plants against natural and accidentally occurring hazards on a basis of 'as chance would have it', and it provides protection against human error by designing the systems and equipment to be tolerant and/or independent of human action (or inaction). This combined approach of gauging the risk by probabilistic assessment and treating the human operators as inconsequential dummies may have some effect in safeguarding the plant against accidents and unintentional human error, but it may prove to be woefully ineffective against intentional and intelligently driven acts of terrorism.

Finally, it should be noted that this paper has considered terrorist attack by aircraft crash, a mode of sabotage that was inconceivable just a few month or so past. We now know that deliberate aircraft crash has to be defended against but what of the next attack, what shape and form will that take and how will plants like Sellafield be defended against it?

Keywords: terrorism, sabotage, nuclear plants

Introduction - Chance of Aircraft Impact

As an example of the modus operandi of a terrorist attack, the mode of attack by the terrorists is assumed to be that of the airliners hijacked by the al-Qaida on 11th September in the United States. That said, a malicious attack on a nuclear plant could arise from armed insurgents, from an external explosive device such as a truck or four-wheel drive vehicle bomb, or via a passive or more directly by an active insider employed within the plant itself.

In the United Kingdom, the Nuclear Installations Inspectorate (NII) regulates the nuclear safety via the regulatory framework of the *Nuclear Installations Act 1965* that is set out in principle by two guidelines the *Safety Assessment Principles* (SAPs)[1] and the *Tolerability of Risk.*[2] *Principles 126* and *127* of the licensing body's (NII) SAPs refer to aircraft impact in the following way:

"...

1) *(P126) The predicted frequency of [accidental] aircraft and helicopter crash on or near safety-related plant at the nuclear site should be determined. The risk associated with the impacts. Including the possibility of aircraft fuel ignition, should be determined to establish whether Principle P119 is satisfied.*

2) *(P127) The calculation of crash frequency should include the most recent crash statistics, flight paths and flight movements for all types of aircraft and take into account forecast changes in these factors if they affect the risk. Relevant bodies should be consulted by the licensee with the object of minimising the risk from aircraft approaching or over-flying the plant.*

. . .” [my insertion]

Principle 119 relates to the anticipated frequency of the hazard, in this case an aircraft crash:-

> “. . .
>
> *(P119) It should be shown for all hazards that the design basis analysis principles and the PSA principles are satisfied as appropriate, unless it can be demonstrated that the frequency of an event being exceeded is less than once in 10 million years, or if the source of the hazard is sufficiently distant that it cannot be expected to affect the plant.*
>
> . . .”

In assessing <u>accidental</u> aircraft crash probability the guidelines and principles set out by the US Department of Energy,[3] are generally adopted. Essentially, this approach assumes some form of loss of control of the subject aircraft, its subsequent deviation from the intended flight path and the chance of it crashing into the target nuclear plant. The nuclear plant is defined as a *crash area* and the parameters relating to this are calculated from the *effective fly-in*, *footprint*, *shadow* and *skid areas* that are determined from established codes.[4]

Applied to a civil airliner operating at altitude and passing along a prescribed flight path, this *a posteriori* probabilistic approach adopts rates drawn from actual crash incidents, yields a very low accidental crash probability.[5,6,7] Essentially, the whole probabilistic assessment outcome is determined by the chance of a very small missile, the aircraft, accidentally hitting a small target, the nuclear plant, located in a very large geographical space. Applying this to nuclear plants suggests that <u>accidental</u> aircraft crash rates are sufficiently low ($<10^7$ per year) to satisfy the requirements of *Principle 119*, that is the hazard occurrence is so remote that it cannot be expected to affect the plant.

For the UK Sizewell B pressurised water reactor (PWR) safety case (of 1987)[8] aircraft crash onto the power station site was identified and considered as an external hazard that had the potential to initiate events that could lead to an accidental release of radioactivity. The expected frequency of impact of all classes of aircraft onto identified vulnerable areas of the power station site was reckoned to be extremely low, at around $7\text{x}10^{-7}$ per year and, of these, impact of aircraft and helicopters less than 2.3 tonnes was not expected to penetrate the containment structures. Thus the design criteria for Sizewell B translated into a construction that provided defence against only the first and lightest level of aircraft impact, that from a small aircraft such as a Piper Cherokee.

Since 11th September Britain's nuclear industry has been unusually tacit about the ability of its plants to withstand terrorist attack. However, a recent example of the position of the world's nuclear safety regulators is given by the Director General, Jukka Laaksonen, of the Finnish Radiation and Nuclear Safety Authority (STUK),[9] who accepts that the lightest level of defence against aircraft crash continues to be acceptable for Finland's two existing, twin reactor nuclear power stations and its proposed fifth power reactor:

> “. . .
>
> *[The] World's nuclear plants are designed on three levels against airplanes. First, against kinds of light airplanes, then against starfighter-type airplanes and then against large commercial airplanes. This design depends primarily on how close to flight-routes these plants are sited and our plants are far from flight routes and we have no fly zones to all planes in the proximity. We have considered the lightest level to be sufficient as a design basis.*
>
> . . .”

The studies for the impact of a heavy military aircraft and commercial airliners, although cited for the Sizewell B assessment were not then and remain unavailable to the public domain. However, it is interesting to note that the title dealing with the military aircraft[10] scenario refers to

> *‘The Effects of Impact Heavy Military Aircraft Adjacent to* ***but Not Directly on*** *the Vulnerable Buildings’*

with the emphasis suggesting that somehow the pilot of this hypothetical aircraft was able to retain some degree of control (and also possess the knowledge of the critical parts of the plant) to avoid the most vulnerable parts of the plant. It is on the basis that the heavy military aircraft would not impact directly, that the Sizewell B operator claims that the likelihood of an unacceptably severe fire or explosion following the impact is sufficiently low to be discounted. In other words, the nuclear industry considers there to be little justification in installing additional features (ie beefing up) to provide aircraft crash resistance.

In fact the NUREG-0800 based analysis permits the introduction of the mitigation that the pilot will retain sufficient control to avoid striking the nuclear plant – for military pilots this is assumed to be for 95% of the time or that, independent of all other considerations, the P_{hit} probability is equal to 0.05.

Of course the probability or chance of the occurrence of a malicious human act, such as the terrorist attack of 11th September, cannot be determined by classical *a priori* probabilistic means. Thus, it is only realistic to apply chance to the success of the attack once it has been initiated. Put another way, applied to the terrorist attack of 11th September the P_{hit} or <u>success</u> rate was 3 out of 4 airborne aircraft, ($P_{hit} = 0.75$).[11] If the aircraft that crashed in Pennsylvania is discounted, the P_{hit} for those aircraft on their target run was 3 out of 3 or 100%. In other words, the hijackers had obtained sufficient flying skills to ensure that, once that the aircraft has been commandeered, the mission would have a high, almost certain rate of achieving its objective. Whereas the military or civil pilot would not be expected to have been trained to identify the vulnerable parts of a nuclear plant (even though it is assumed that the pilot will strive to avoid certain parts of the plant), it would be in the hijacker's interest to identify the most vulnerable parts of the selected target. Hence, the same NUREG-0800 mitigation applies, but in this case in reverse with the terrorist intent of striking the plant with, perhaps, a P_{hit} of

95% of success once committed to the final run to the target.[12]

The imposition of notional restraints such as no-fly zones nearby nuclear plants are to no effect once that an aircraft has been commandeered and the terrorist attack is underway. If the attacking terrorists fly to the targeted plant by line of sight (apparently the case for the World Trade Center), then visual contact at cruising altitude is achieved at about 30 plus miles which leaves but an impracticably short time scale (4 to 5 minutes) for the authorities to detect, intercept, interrogate and implement the appropriate remedial action to thwart the attack.

Forecasting the Possible Outcome & Consequences of a Terrorist Attack

Because an accidental crash of a civil airliner on some part of a nuclear site would be reckoned, on the basis of the established assessment routines, to be a very remote event it is likely to be considered beyond the design basis. However, *Principle 28* of the NII SAPs[1] requires fault sequences beyond the design basis that have the potential to lead to a severe accident to be considered and analysed (by bounding cases[13] if appropriate) and there may be specific requirements for protection of the plant against sabotage which are not published.[14]

In other words, if it is acknowledged that an accidental aircraft crash could lead to a very severe radioactive release then, however remote the probability of this event, there is a requirement that the consequences be identified and assessed. Put another way, this is a *consequence analysis* approach that disregards any offset from the probabilistic value of a foreseeable event happening. If the aircraft crash is an act of sabotage then the probability must be assumed at unity ($P_{hit} = 1$) and the event considered only in terms of its consequence mitigation.

Application to a Nuclear Power Station Site

The SAPs *Principle 28* particularly applies to the containment of the plant, it being a requirement to *"identify the failures which could occur to the physical barriers to the release of radioactive material"*, although it is not clear whether *Principle 28* has been applied to all of the systems and processes within a nuclear power station or, indeed, to all types and ages of nuclear power stations. Also, if *Principle 28* has been applied, it is not clear whether i) the general premise that the plant containment would survive the impact and fuel burn or, and as for the Sizewell B nuclear safety case, ii) that the chance of an accidental air crash is considered so remote as to be entirely incredible.

The uncertainty here is that if it is acknowledged that a terrorist attack by aircraft crash is now, *a posteriori* (that is an established external hazard) are the plant operators now required to review and amend the nuclear safety case in account of this?

Returning to Finland and its preparation to select the type of reactor plant for its fifth reactor, there the safety regulator seems to have conducted preliminary reviews of plant types, setting these again *'new safety requirements'* noting that:[15]

". . .

> *STUK has not made facility-specific assessments of how the facility concepts presented in the application meet the new safety requirements. According to STUK the structural designs of all the plant concepts would require some modification. However, none of the proposed power plant types would be need to be rejected based on current knowledge.*
>
> .
>
> . ."

SAPs Principle 28 - Consequence Mitigation

First, it follows that the design and construction of the buildings of these sites were likely to comply with the regulations and good practice of the times, being considered then *'fit for purpose'.*[16] So, even if the designers of the day had then included within the building and containment designs (and processes within) features resistance to aircraft crash, the assessment would have related to the types of aircraft flying at that time. Similarly, the need or priority to incorporate such features would have sensibly related to the density of aircraft traffic at that time, that is the probability of a crash event. Second, for those plants designed and regulated from a probabilistic basis, it is very doubtful indeed that any intentional aircraft crash resistance was built into the system, that is not just for the building structures and physical containments, but also on the resistance of safety equipment to resist impulse loading and the fire associated with aircraft crash.

Put another way, most of Britain's nuclear plants were designed and set down in the 1950s, 60s and 70s when commercial aircraft were typical of the relatively small size of a Vickers Viscount and similar. Today, there are no Viscounts in commercial service yet all of the nuclear plants of those bygone times remain, most continuing in operation.

These two inconsistencies alone suggest that it would be impracticable for the world's nuclear plant operators to modify much of the existing plant so that it would be reasonably guaranteed to survive an aircraft crash. The severity of an aircraft crash might drive through and render ineffective the normally accepted physical systems that serve to limit the consequences, such as safe shutdown, continued availability of utilities, adequate containment integrity and on- and off-site emergency preparedness. If so, the accident would still have to be 'managed' by improvising the use of other surviving systems and resources, which requires an increased reliance upon operator intervention because accident management strategies must be implemented by plant personnel.

One area of doubt here is that nuclear plants are designed to withstand, as far as is practicable, specified external hazards such as earthquakes, flooding, etc., but, this being so, this defence is quite scenario-specific and the capability of certain items of equipment to survive depends not only on the custom engineered resistance to particular scenarios but, importantly, on the diversity of function of the safety systems and equipment involved. The point here is whether the diversity of the installed equipment is sufficiently broad to resist a common mode failure across all of the equipment and systems that could be triggered by aircraft impact, fuel explosion[17] and the subsequent fire.

Also, it is doubtful that the outcome of a *consequence analysis* could be practicably implemented to provide an effective consequence mitigation management regime. Moreover, accident management, even if performed as planned, might prove ineffective leading from one severe accident sequence to another just as hazardous and it may, in certain rapidly developing situations, be counter-productive.

The Impact and Ensuing Fire of an Aircraft Crash

Aircraft, for all of their speed and power, are relatively fragile structures. The 190 or so tonnes of each Boeing 767 that crashed into the South and North the towers of the World Trade Center may have provided a colossal kinetic energy but the wings and fuselage would have shredded almost immediately, leaving just the compact masses of the engines and a few solid spars and undercarriage frames in the role of very energetic projectiles to penetrate the building structure. Accompanying this high-energy impact was the release of the 80,000 litres or so of aviation fuel, partially vaporised that erupted into fireballs to ignite flammable materials in the vicinity.[18] Vaporised and unburnt fuel would have been squeezed into building voids by the expanding flame and pressure fronts and the remaining fuel would have gushed into the internals of building, spreading downwards through buckled and holed floors. As the tragedy unfurled it was clear within minutes that about ten floors of each of the towers of the World Trade Center were burning furiously, so intensely that the structures buckled and progressive collapse commenced on the South Tower within one hour of the aircraft impact.

Now that a full analysis of the collapse of both the World Trade Center towers and the Pentagon has been published,[19] it is clear that both impact and fire phases of the crash played active roles in the destruction of the buildings. The initial impact would have destroyed or weakened the structure of the buildings and the immediately following fire was of sufficient temperature to ignite all flammable materials within, which provoked further structural member buckling and damage leading to catastrophic structural failure.

Application of an Aircraft Crash to the Engineered Structures of Nuclear Power Plants

Obviously, the effect and outcome of an aircraft crash and fuel explosion/burning on any one of the active plant building or processing/storage area would be subject to how each of the individual target buildings would perform under the impact and fire conditions.

As a result of impact (kinetic) energy is transferred from the aircraft to the building.[20] The energy transferred is absorbed by the building components in the form of strain energy whilst each component is deforming elastically and beyond up to the point of permanent yielding. The impact can be segregated into two regimes: First, at the moment of impact the aircraft can be considered to be a very large but relatively 'soft' projectile which, by self-deformation' will dissipate some fraction of the total kinetic energy being transferred during the impact event. Second, some components of the aircraft will be sufficiently tough to form rigid projectiles that will strike and commence to penetrate, again by kinetic energy, components of the building fabric and structure.

The first of these damage regimes involves quasi-impulsive loading, so the response of the structure is obtained by equating the work done by the impacting load to the strain energy produced in the structures. Setting aside localised damage in which individual structural components are removed (blasted away), the most probable failure mode of the structure overall is that of buckling and collapse in response to the impact. The types of building structure featured at nuclear power plants, for example the radioactive waste and spent fuel buildings, would not withstand the impulse magnitude delivered by a crashing commercial aircraft.[21]

For impact damage the aircraft, more particularly parts and components of it, have to be considered as inert projectiles. The energy transfer upon impact relates to the kinetic energy (KE) and the key parameter in determining the target (building component) response is the kinetic energy density which relates the KE and the projected area of the projectile. In terms of projectile velocity, a diving civilian aircraft is unlikely to exceed 500 knots so the damage mechanism falls below the so-called hydrodynamic regime where the intensity of the projectile-target interaction is so high that a fluid-to-fluid damage mechanism prevails (as utilised by tungsten tipped and depleted uranium sarab or long rod penetrator armour piercing rounds).[22] In the sub-hydrodynamic regime more conventional strength of materials characteristics (ie strength, stiffness, hardness and toughness) will determine the penetration mechanism.

For uniform, elastic materials, such as low carbon steel used in steel-frame construction such as diesel generator sheds, radioactive waste stores and, sometimes, irradiated fuel storage buildings, a good first estimate of the penetrating power of a projectile can be obtained from the Recht equation which, for certain hard components of the aircraft engines, could be as high as 200mm.[23] For a steel framed industrial building structure, typical web and flange thicknesses of the steel section girders and beams is typically about 20 to 40mm so, even with penetrator break up, this and other projectiles would be more than sufficient to structurally damage, if not catastrophically collapse the building steel frame.

The failure of reinforced concrete (rc) to ballistic loading applies to the different ways in which this common building structural material is used: For very thick walled structures the concrete is considered to be a semi-infinite mass, for concrete walling and flooring (and roof) slabs the account has to be taken of the flexure of the slab, and to prevent scabbing (where the back face of the concrete surface detaches) the reflective characteristics have to be modelled. The first two of these applications are important in respect to the whole structure remaining intact, and the last that in even where complete penetration is not achieved, the detached scab can form a missile in itself damaging and/or disabling safety critical plant within the concrete containment. The derivation of the ballistic loading of ferro-concrete (steel reinforced concrete) structures is a little more empirically derived,[24] although even with broad brush assumptions about the detailed design of the ferro-concrete structures the hardened projectile striking most of the concrete structures of a nuclear power plant would achieve full penetration. For example, a glancing impact on a typical rc framed building would be sufficient to possibly penetrate the rc roof slabs which are not practicably greater than 400mm thickness, (because of selfweight loading considerations over the 4m spans).

The point here is that the building structures of a nuclear plant require to maintain complete containment during an aircraft crash because even relatively small penetrations will permit the inflow of aviation fuel with the almost certain fire aftermath which would, in itself heighten the release and dispersal of any radioactive materials held within the building structure.

For the purposes of this paper, it is quite reasonable to assume that the building containment would be breached – this is likely to be a justified assumption because of the absence of any extraordinary civil engineering features visibly incorporated into the building design. On this assumption, once that the building is breached it may be that the particular process and/or substances stored within will add to the damage, by explosion, and ferocity of the fire (flammables).

For a typical nuclear power plant, the following outline scenarios might arise: -

Irradiated Fuel Storage: Of the covered fuel ponds, if the roof structure was penetrated and the pond wall structure breached, then loss of pond water and aviation fuel fire could lead to a breakdown of the fuel cladding and fuel itself, resulting in a high release fraction of fission products, possibly mixed with emulsions of the aviation fuel. The fuel pond radioactive inventory depends on the degree of irradiation of the fuel (the burn-up) and the post in-core period, although the quantity of fuel might represent (in mass) 7 to 8 times, or more, the reactor core load.

Zircalloy clad oxide fuels provide opportunity for an exothermic and self-sustaining zirconium/steam (or air) reaction at elevated temperatures that will result in, obviously, failure of the fuel cladding and increased oxidation of the exposed fuel pellet surfaces, with the hydrogen liberated from the oxygen stripping and exothermic chemical reaction $Zn+H_2O$ providing a hydrogen explosive atmosphere, with the accompanying radioactive release of spent fuel fission products potentially very significant.[25] For the UK Magnox nuclear power stations, and for certain research reactors, the magnesium alloy cladding and the base elemental metal fuel are pyrophoric in air which could result in a very efficient release of the reactor core or spent fuel pond inventory.

A crashing airliner, displacement of the fuel pond water and introduction of burning aviation fuel could result in a very significant radioactive release from the irradiated fuel pond. The subsequent dispersion range of the airborne carried radioactivity could be much enhanced by the high thermal energy involved (plume height) and combination of fission products with emulsions of the aviation fuel and its products of combustion.

Intermediate Radioactive Wastes: The radioactive inventories and chemical make-up of the stored radioactive wastes at nuclear plants sites is known and because of the dilemma over failure to find a national radioactive waste repository for high and intermediate level categories of radioactive waste such wastes will accumulate at the individual nuclear sites for the immediate and interim futures.

Certain nuclear sites carry a high burden of radioactive wastes. At Sellafield, for example, there are very large volumes in store, some of which are flammable in themselves, such as the 1,000m^3 or more of contaminated reprocessing solvent (odourless kerosene) which could add considerably to the aftermath fires of an aircraft impact.

Operational Nuclear Reactors: The range of potential outcomes for operational reactors subject to terrorist attack is large.

Obviously, a direct impact on the reactor locality, breaching the reactor pressure vessel and/or the primary coolant circuit would most probably result in a radioactive release into and through the secondary containment systems that would have also been breached by the impacting airframe. Other safety-critical equipment of operational nuclear power plants include the electricity supply grid connections and the emergency diesel electricity generators, both of which provide essential electrical suppliers for safety systems, reactor cooling and heat sinks, loss of which, particularly effective core cooling, could result in containment challenging events developing in the reactor core.

The main conclusions that can be drawn from these scenarios are that:-

a) None of the UK's nuclear reactors has a containment which has been specifically designed to resist aircraft attack, other than at Sizewell B where the reactor secondary containment dome is designed to resist an accidental impact of a light aircraft;

b) none of the radioactive waste and spent fuel facilities, at the nuclear power plants and at BNF:L Sellafield, could withstand the directed impact of a fully loaded commercial airliner; and

c) many of the radioactive waste and fuel storage facilities, again at the nuclear power plants and at Sellafield, contain massive amounts of radioactive material available for suspension and dispersal in the aftermath of a terrorist attack.[26]

Conclusions

This paper set itself three objectives. These were

1) is there sufficiently detailed information available in the public domain for a terrorist group to plan an attack with sufficient confidence of success;

2) does the regulatory safety case requirement include for <u>accidental</u> aircraft crash and, if it does,

is this sufficient to safeguard against <u>intentional</u> aircraft crash; and

3) could the plant's systems and processes be modified and prepared to withstand such an intentional attack and, if so, how much of this defence would depend upon accepting intentional aircraft crash as inevitable, thereby relying almost totally upon consequence management to mitigate the outcome.

Information Accessibility: Using the United States and the United Kingdom plants as yardsticks, it is relatively straightforward to obtain all of the information required by simply accessing publicly available documents. Ministries and agencies of central government publish most of these sources of quite detailed information, and local authorities maintain records of planning applications that include details of extant as well as proposed plants and buildings. These records and documents are readily accessible, it being possible to obtain copies directly from the originating department of documents that dated back to 1996 and earlier.

Also, there are a number of *'storehouses'* of related information. Local and national, and international environmental (and other) groups hold pools of information that they have accumulated over the years. As example, one local group was able to provide photographs of locations deep within the BNFL Sellafield fuel reprocessing site, fully detailed engineered drawings of buildings, and scaled site maps that included the location of essential services, are available for the Sizewell B PWR reactor from the Construction Report prepared for and published at the Public Inquiry.

When responding to requests for information and documentation, both HMG and the relevant local authority did not enquire to what purpose the information was required and, during my (Large & Associates) requests, there seems to have been no double-checking of the bona fides and identity of the enquirer.

Surprisingly, although as a result of the 11th September attacks the US Nuclear Regulatory Commission closed down all of its Internet web sites while it reviews the contents, web pages relating to Sellafield (HMG, BNFL, etc) remain open and accessible.

Aircraft Crash and Design Basis Threats: Although this paper centres around an <u>intentional</u> aircraft crash, a future terrorist attack against a nuclear plant might be in the form of some other external, man-made hazard. However, here I have only considered aircraft crash in any detail, although a future terrorist incident might involve, for example, a truck bomb driven close to or actually into the plant secure area.

The requirement that aircraft crash, irrespective of the forecast accident frequency, be accounted for in the regulatory safety case was not introduced until 1979 for nuclear reactors and 1983 for chemical separation and nuclear fuel plants such as those at Sellafield - examples of where the nuclear industry have taken this into account, such as for the Sizewell B PWR, are almost dismissive of the risk solely on the basis that the calculated frequency renders such an <u>accidental</u> event to be entirely incredible and, hence, there may have been little incentive to include for such a remote event in the design.

For other Design Basis Threats (DBTs) the US Nuclear Regulatory Commission requires nuclear plant operators to submit to *force-on-force* trials simulating intentional malicious actions. Since 1991 the NRC has conducted 91 trials or *Operational Safeguards Response Evaluation* tests, of which about 45% of the tested nuclear plants failed. Most disturbing is that three plants tested shortly before 11th September, Farley, Oyster Creek and Vermont Yankee, were the worst on record. In another assessment, the NRC notes that between 15 to 20% of US nuclear plants would sustain safety critical levels of damage from vehicle bombs accessing close to the supervised boundary of the plant.[27]

Preparedness in Britain: In the past, although some British nuclear plants have been subject to mock attack exercises nothing on their vulnerability and/or performance has been published. Recently (May 2002), however, Bradwell nuclear power station was subject to some form of trial which involved the local authority emergency planning resource and which must have involved the central government Department of Trade's Office for Civil Nuclear Security (OCNS).

Apparently (because nothing is publicly available), OCNS has evolved a new procedure to assess security threats which are to be incorporated into a Design Basis Threat document which is to be the key planning aid for the plant operators. The DBT will provide intelligence about the 'motives, intentions and capabilities'[28] of potential adversaries against which the plant operator is to 'beef-up' the plant management, contingency planning and physical security measures. Once all of this is in place, the Director of the OCNS will evaluate the robustness of Britain's individual nuclear plants, making this publicly available in its first annual report.[29]

At governmental level there is the recently formed Cabinet sub-committee referred to as the Chemical, Biological, Radiological and Nuclear (CBRN). The role of CBRN is to review the contingency arrangements in place to protect against terrorist attack, although its findings are classified restricted and above, and nothing is publicly available on its membership and how and to whom it communicates its recommendations.

At local government level local authorities are presently preparing off-site plans as required by the *Radiation (Emergency Preparedness & Public Information) Regulations* (REPPIR). For this the nuclear plant operator is required to prepare a Report of Assessment upon which the Health & Safety Executive determines the need and coverage of any off-site emergency planning. REPPIR was prepared and enacted before the events of 11th September so, not surprisingly, it is silent on the specific need to include DBTs in the Report of Assessment. The extent to which realistic DBTs have been included by the operator and, importantly, how the limited resources of local authorities can be marshaled as effective countermeasures or, at least, to mitigate the potential consequences has yet to be made publicly available, although all will be revealed by off-site plan implementation deadline of 20th September 2002.[30]

Like many other nuclear countries, Britain has been jarred into action by the events of 11th September. New committees have been formed, assessments are being made and there is now, via REPPIR, a real opportunity to put in place, resources permitting, effective emergency planning and consequence management measures.[31]

However, it has to be acknowledged that modifying the existing plants to improve their physical invulnerability is just not practicably feasible. In place of this, there must be effective intelligence gathering on the ground in advance of any planned attack and this must be communicated to the operators and the emergency planners.

Now that we are beginning to learn that although informed in advance of the threat, the Bush administration was unable the thwart the 11th September attacks. A similar failure in acting upon gathered intelligence could not be tolerated again, particularly if it was believed that a nuclear plant had been identified as a target.

Defending Nuclear Plants - Consequence Management: Nuclear plants are almost totally ill-prepared for a terrorist attack from the air. The design and construction of the buildings date from a period of over 50 years, many of the older buildings would just not withstand an aircraft crash and subsequent aviation fuel fire, some buildings, now redundant for the original purpose, have been crudely adapted for storage of large quantities of radioactive materials for which they are clearly unsuited, and the design of the most modern plants on the site does not seem to provide that much defence (in terms of containment surety, dispersion of stocks to different localities, and segregation of hazardous materials) against an aerial attack.

It would not seem to be practicable for each and every building and process at such nuclear plants to be modified to provide adequate protection against aircraft crash. The investment requirement would be enormous and the practical difficulties challenging indeed – many of the processes would have to be relocated, possibly to underground caverns and bunkers, which in itself might introduce other safety related detriments.

If a terrorist group planned to <u>intentionally</u> crash an aircraft onto a nuclear power station then the probability of the event becomes unity and it is inappropriate to mitigate the chance of such an intentional attack occurring by probabilistic based assessment. Considering an intentional, terrorist driven aircraft crash as a certainty, rather than as some remote probability, requires the event to be assessed in terms of its consequence management alone and this consequence management is the only form of mitigation available. In other words, there are no practicable measures that might be implemented on site to provide a defence in depth to avert such an event.

However, the idea that a severely damaging event, arriving like a bolt out of the blue, could be *'managed'* by improvising the use of other systems and resources is doubted, particularly because ad hoc decisions and actions (taken in unpracticed and highly stressed situations) might lead from one severe condition situation to another just as hazardous.[32]

References

---

[1] *Safety Assessment Principles for Nuclear Plants*, NII, Health & Safety Executive, May 2000 first introduced for nuclear reactors in 1979 and for nuclear chemical plants in 1983

[2] *The Tolerability of Risk*, Health & Safety Executive 1988, revised 1992

[3] *Accident Analysis for Aircraft Crash into Hazardous Facilities*, DOE-STD-3014-96, 1996 see also for practical application *NUREG-0800, Section 3.5.1.6 Aircraft Hazards*, Nuclear Regulatory Commission, 1981 which suggest a crash rate in the absence of other data to be $3.66 x 10^9$ per flight mile.

[4] STD-3014-96, US Department of Energy, 1996

[5] For example see *Evaluation of Aircraft Crash Hazards for Nuclear Power Plants*, Kot C A, et al, Argonne National Laboratory, 1982 which gives a chance of crash into a nuclear plant 11.5 miles to the south of an air corridor at 33,000 ft to be about $2.36 x 10^7$ per year and *Evaluation of Air Traffic Hazards at Nuclear Power Plants*, Hornyik K, Nucl Technology 23, 28, 1974

[6] *Aircraft Impact on Sizewell B, Part 1 Safety Involvement of Buildings on Site*, PWR/RX774 (pt 1) 1987

[7] *Sizewell B PWR Supplement to the Pre-Construction Safety Report on External Hazards, Aircraft Crash*, CEGB Report No GD/PE-N/403, 1982, *Aircraft Impact on Sizewell B*, Part 2(a), *The Effects of Impact of Heavy Aircraft Adjacent to but not directly on Vulnerable Buildings. (b) Light Aircraft on the Vulnerable Buildings*, PWR/RX774 (Pt 2), 1987 and *Aircraft Impact on Sizewell B* Part 3 *Fire Following Aircraft Crash*, PWR/RX774 Part 3, 1987

[8] *Sizewell B PWR Preconstruction Safety Report*, Chapter 3, November 1987

[9] Finland is currently planning a fifth nuclear reactor and has consolidated this position since the 11 September incident, with a final parliamentary decision expected about June 2002. Transcript of interview by Finnish Broadcasting Company, A-Studie 12 November 2001 – the transcript is in English and there is no authority on the accuracy of any translational/transcription.

[10] Military aircraft are considered as exceptional because they are not restricted to fixed air corridors and can effectively freely roam the skies

[11] Although it is acknowledged that this is drawn from a statistically insignificant grouping (just the 11th September data), the assumptions for the reliability of military pilots to avoid the vulnerable parts of the building must also be drawn from a lean set of data.

[12] However, it should be noted that homing in and striking on a low target (ie a low rise building) would present greater difficulty to a novice pilot than that of striking a large high rise structure.

[13] A *'bounding case'* is where the different faults and fault sequences may be grouped together in that the consequences for any fault

---

sequence is as least as severe as every member of the groups of fault sequences to which it is bound.

[14] For example, in the United States the *US Code of Federal Regulations Requirements for Physical Protection of Licensed Activities in Nuclear Power Reactors Against Radiological Sabotage*, S55, PT73 applies although this includes little protection against deliberate aircraft crash. In the UK there are controls applied to the proximity of aircraft to nuclear plants with Statutory Instrument 2001 (1607) The Air Navigation (Restriction of Flying) (Nuclear Installations) Regulations 2001 came into force on 11 May 2001 – this prohibits flying below specified height of 2,200m above circular areas defined for Sellafield for a radius of 2 miles at OS 542505N 032944W.

[15] *Preliminary Safety Judgement on the Application for a Fifth Nuclear Power Plant*, STUK, December 2001

[16] *The Building Regulations 1976 (as amended)* – first introduced by Section 61 of the Public Health Act 1936 the Building Regulations were made for the following broad purposes a) securing the health, safety and welfare of people; b) furthering the conservation of fuel and power; and c) preventing waste, undue consumption and misuse or contamination of water. It is sufficient to note here that the regulatory system of building control in the United Kingdom, *The Building Regulations*, centres about protection of the occupants of buildings, particularly in the event of fire, inasmuch that sufficient means of escape, compartmentisation to inhibit the spread of smoke and fire, and time for escape shall be provided. In this approach it is left to the building designer to specify specific types of loading, etc., that might apply to the building during the course of its function and use, so other that standards set down for floor, wind, snow, etc., loadings and, since the late 1960s, safeguards against progressive collapse for buildings of five or more storeys, nothing specific is prescribed for external/internal hazards including aircraft crash.

[17] Commercial jet fuel typically has a heat of combustion of about 38 MJ per liter against, for comparison, 4.2 MJ of energy for the same mass of TNT. If conditions are right, some part of the combustion process of the aviation fuel during the impact could be in the form of a fuel-air explosion which could be quite violent, generating a high energy blast wave which could add to the destruction (locally and in addition to the impulse loading of the impact).

[18] The fuel load and aircraft mass could be significantly larger. For example, applied to Sellafield there are about 250 flights of Boeing (Jumbo) 747 airliners per week passing over the North West region of England. Flying from Amsterdam a Boeing 747 would commence its flight with about 175 tonnes of aviation fuel and fuel consumption for taxiing, take-off, climb and cruise to Sellafield would leave about 155 tonnes of fuel at impact.

[19] Now published the official report produced by the American Society of Civil Engineers (ASCE) for the Federal Emergency Management Agency (FEMA), May 2002.

[20] Just on the basis of kinetic energy alone the three levels of aircraft crash referred to by the STUK regulator increase from Level 1 (light aircraft) to Level 2 (Jet Fighter) to Level 3 (Commercial) airliner in the ratio 1 to 50 to 1500 or that the energy available from a crashing commercial airline (impact alone) is 1500 times that of a light aircraft.

[21] The maximum impact before yielding commences is given by

$$i_r = [2Lim/En]^{0.5} \partial_y/Ah$$

which (adopting conventional notation) for the a typical rc construction, with a roof slab load per column assumed at 35t, the structure yields at about 1,750 Pa-s. The impulse force arising from a crashing aircraft of, say 200 tonnes all-up weight considered impacting over its projected front end fuselage area (about 30m^2) with the event lasting over the entire collapse of the fuselage length, gives an impulse force of about 20,000 Pa-s or about x10 the yield strength of the typical rc structure described above.

[22] At projectile impact velocities below 1000m/s all impacts are sub-hydrodynamic – at 500 knots the closing velocity at impact would be approximately 260m/s.

[23] After R F Recht, *Ballistic Perforation Dynamics of Armor-Piercing Projectiles*, NWC TP4532, 1967. which, for a blunt nose ogive, is

$$x = 1.61M/(bA)[V-a/b\ln([a+bV]/a)]$$

where *a* and *b* relate to the material properties of the target, M is the mass of the projectile and V the projectile closing velocity. For an aircraft impact, if it is assumed that a sufficiently robust penetrator will present itself in the form of a main turbine shaft of an aero engine which, with its blades and other attachments, might represent a mass of 0.25 tonnes of 150mm projected diameter (stub end of shaft), typical strength of materials properties give $a = 2.10^9$ and $b = 10.10^6$, so that the final penetration thickness into a steel element (ie a building stanchion) is about 200mm.

[24] *MOD Assessment, Strengthening, Hardening, Repair and Demolition of Existing Structures*, Army Code No 71523, MoD 1992 which, for the same missile adopted for *Footnote 23* the slab penetration is about 1,100mm.

[25] *Technical Study of Spent Fuel Pool Accident Risk at Decommissioning Nuclear Power Plants*, NRC October 2000

[26] For example, at Sellafield there is in store, in powdered dioxide form, approximately 72 tonnes of plutonium-239 which has been recovered over the years from fuel reprocessing – this plutonium stockpile is store in two adjacent building details of which have been readily accessible from the local planning authority.

[27] Lyman E, *Terrorism Threat and Nuclear Power: Recent Developments and Lessons to be Learned,* Rethinking Nuclear Energy and Democracy after 09/11, Int Symp, PSR/IPPNW Switzerland, Basel April 2002)

[28] Sunil Parekh, Assistant Private Secretary to John Denham, Home Office Minister, 10 May 2002

[29] The DTI OCNS first report has now been published but it contains no details whatsoever about the performance of the individual nuclear power plants, although it notes that it, itself, is experiencing staffing difficulties that does not permit it to carry out its function completely.

[30] By 20 September or six months after the HSE has served notice to the relevant local authority – at the moment the HSE seems to be running about 3 to 4 months late on these notices so implementation for many sites would not be expected to until the new years of 2003.

[31] There is considerable confusion, or so it seems, relating to the emergency limits for radiation exposure for individuals expected to support the local authority off-site emergency plan. For example, local authority off-site plans assume that the three emergency services will attend without restriction. Of these, the firefighters have their own nationally agreed incident exposure limits (50mSv and 100mSv for lifesaving), the Ambulance Service Association (representing all 35 UK NHS ambulance services) has a *'zero tolerance'* of radiation exposure for its crews and paramedics, and the police forces do not provide specific training and individual officers are not issued with any means of personal dosimetry – only the firefighters seem to be aware of the need to have a competent person overseeing the radiation exposure of individual firefighters and crews. The incredible situation of having a number of competent persons, each permitting different exposures is possible under the *Regulations.*

The differences in the dose limitation systems (where such exist) could result in non-attendance of the ambulance crews, definitely staged withdrawal of firefighters at their own preset limits, that is well before local authority employees reach the HSE's recommended radiation exposure limits (100mSv and

---

250mSv for lifesaving), leaving just the police alone to lead the countermeasures without the support of their emergency services colleagues.

On its part, the HSE is presently recommending emergency dose limits of 100 and 250mSv, the latter for life saving, for those individuals participating in the off-site plan but this seems to give no account of high risk nature of the employment of firefighters and police officers (ie in account of the total risk including that encountered in the course of non-nuclear activities) and the fact that the majority of local authorities could not be expected to train and equip each of their employees participating in the emergency with real time personal dosimetry equipment.

[32] This paper has concentrated on nuclear site plants and processes on a nuclear site itself. It should also be noted that a nuclear plant depend upon the continuous import of services, particularly electricity and mains water, to maintain safety on the site, and if imported electricity supplies fail solely on the on-site emergency plant supplies. These imported services (the national grid electricity lines, emergency generators and water pipelines may also be susceptible to terrorist attack.