INSIGHT

Sizewell B: Fact or Fiction?

Anybody who keeps an eye on UK newspapers will have noticed that in the last month, computer viruses have hit the headlines once again. The cause of this wave of media publicity was the infection of computers at the *Sizewell B* nuclear power station. The story, with perceived danger to the public, nuclear power, and computer viruses, had all the elements necessary to be highly newsworthy, and much of the portrayal bordered on the hysterical. The key question was whether a virus could compromise safety at the plant.

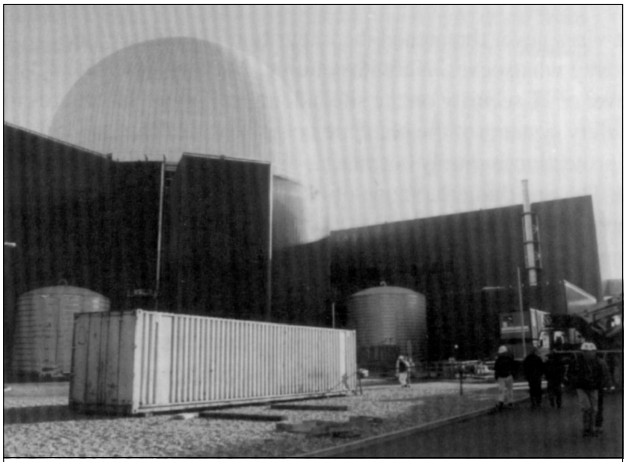
Power to the People

As one drives up the A12 from London it soon becomes obvious that a large project is underway at *Sizewell* - the signs for the '*Sizewell B* construction traffic' start before Ipswich, and lead the traveller down increasingly small roads until he eventually arrives at *Nuclear Electric's* newest reactor site. The plant is situated on the east coast of England, near the sleepy town of Leiston: at first glimpse one has no idea of the size of the project. A number of power lines converge on the station from the surrounding area, and the white dome of the containment building stands out from the flat Suffolk countryside.

Upon my arrival at the plant, I was directed to my parking place beneath one of the towering pylons which was humming and crackling above me, and the true scale of the project began to dawn: at *Sizewell*, B clearly stands for big!

Check your Disks Here

When anyone enters the site they have to pass through a security checkpoint. Here, the visitor is asked if he is carrying any computer media, and if so, the disks are checked for viruses. Somewhat dog-eared posters adorn the doors of the security checkpoint, reminding users that 'All computers must be checked' and appealing to everyone to 'B Safe' - the system has clearly been in place for some time, rather than just put up after the recent virus attack.



Sizewell B's containment building, just one of the many different safety features built in to the reactor

The machines which became infected with the Yankee virus were not part of the controversial Primary Protection System, but of the construction team's *Local Area Networks* (*LAN*). 'Let me explain the different systems we have here,' said Dave Hollick, Site Manager. 'There are the construction computers, and split off from them are the computers which actually control the site. The construction computer systems are linked into a *LAN* running *OS/2*. Another 120 dumb terminals link into the *Nuclear Electric* mainframe system based off-site. So the virus never affected the control systems. What we have here is basically a standard office system, and it was this which became infected.'

'The 29th of June was the date it happened. We had a full investigation of the incident, and all members of the team were re-inducted. We then got some press coverage locally in the *East Anglia Daily Times*, and thought that was the end of it,' explained Hollick. 'The virus infected the *LAN* and we found out on the day it became infected - even if the trigger hadn't been so obvious, we would have found out the next day when people logged on to the system.'

The site policy is very strict. Every incoming disk should be checked by security at the door, although with a maximum of 5,000 people working on-site at any one time, this can be a gargantuan task. 'Each of the construction computers is checked for viruses when anyone logs on to the network, and since the Yankee outbreak, we have installed a new tool, *PC Guard*, so that it is impossible to run unauthorised software from floppy disks,' Hollick adds. 'We have three different virus scanners: *Dr Solomon's Anti-Virus ToolKit, Central Point Anti-Virus* and *Norton Anti-Virus*. Computer security is something which we take very seriously.'

With so many different people using the site, it was probable that sooner or later, a computer would be infected by a virus. In this eventuality, would there be any threat to the safety of the plant? 'Absolutely not!' exclaimed Len Green, Press Officer. 'The safety systems of the plant aren't run on PCs. If you are using mission critical software, you have to ensure that computer corruption cannot make things unsafe.'

Fail Safe

The easiest way to minimise the effect of computer error is having a large number of backup systems. The computers which actually control the *Sizewell* plant have the ability to shut the reactor down completely - was Green certain that they were not susceptible to virus infection? 'Yes. The

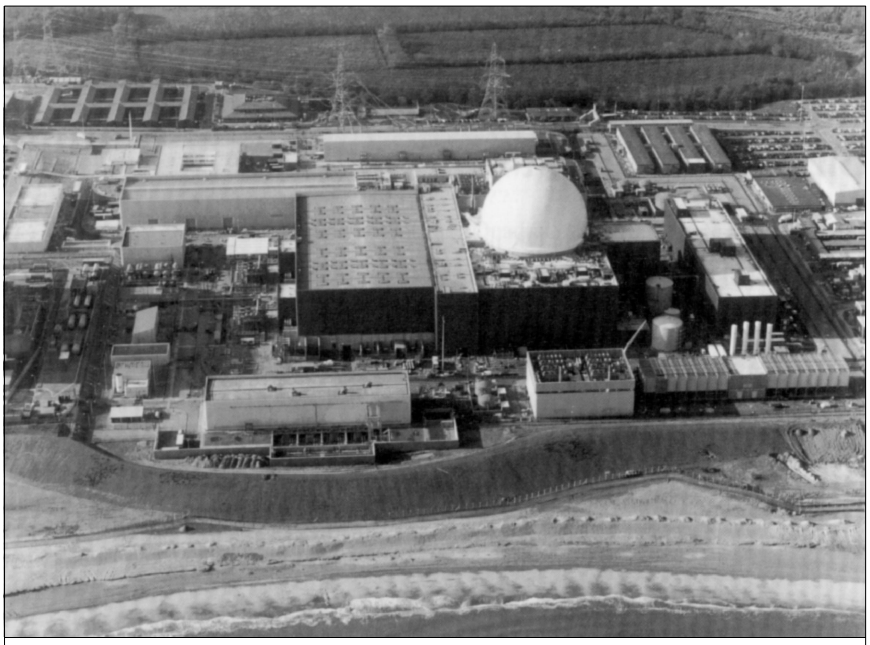
software itself is blown onto PROMs, and then that's that. An operator cannot add new code to the system. The most that can be done is that calibrations can be changed - something that is necessary in a system, however it is controlled.'

To anyone designing failure sensitive systems, the following precautions will be very familiar. The different parts of the system work on the principle of multiple layers of defence. The reactor itself is controlled and monitored by a dedicated system know as *WISCO* (*Westinghouse System for Centralised Operation*). This system is backed up by the reactor protection systems, the Primary Protection System (PPS) and the Secondary Protection System (SPS). It is the PPS which seems to have caused the most controversy. These protection systems would be used to shut the reactor down in the event of an emergency. How has *Nuclear Electric* made certain they are safe?

The PPS consists of over 100,000 lines of computer code. Although the system cannot possibly be infected by a computer virus (it is stored only on read-only memory), there is always the possibility of bugs. 'Let us assume for a minute that the Primary Protection System completely malfunctions,' explains Green. 'Imagine a fault develops and the system ups the power instead of shutting it down. At this point the SPS cuts in. That doesn't rely on computers at all, and cannot be overridden by an operator. Every safety critical feature of the plant is backed up: we don't rely on any one system alone for safety.'

Media Attention

Given that safety at the plant was never compromised, how does Green feel about the way in which the story was portrayed? 'The frustration is that there are plenty of people who understand computer systems, who don't understand the way in which nuclear power works. These people don't know about the multiple fail-safes which we have.'



Hollick: 'We have three different virus scanners: *Dr Solomon's Anti-Virus ToolKit*, *Central Point Anti-Virus* and *Norton Anti-Virus*. Computer security is something which we take very seriously.'

'I'm still receiving calls from all over the place about this virus outbreak. I had a call from German television this morning - and the whole thing is a non-story!' With perfect timing the telephone rings… it is another call from the press. 'Things have been taken out of context, and the way in which it has been portrayed just has not been reasonable. I *understand* people wanting to know more - I want people to know more - but the system has not had a fair hearing. It makes my blood boil!'

From the half day spent at *Sizewell*, it certainly seems that *Nuclear Electric* takes the threat of viruses seriously, and is taking the right steps to prevent them spreading. 'What's the story? I carry this thing around,' Green holds up his laptop computer, which is covered in copious amounts of 'Virus Checked' stickers. 'I'm getting stickers at every location to show this computer has been virus-checked - look at it, it's covered. We take computer security very seriously here. We've already dismissed an agency engineer for using unauthorised software. I know that if I cut across established procedures, my job is on the line! That's been demonstrated.'

The Last Word

It is clear that the Yankee virus never threatened the integrity of the *Sizewell B* computer systems in any way whatsoever. Notwithstanding, *Nuclear Electric* decided to increase the level of IT security on the site, adding still more safeguards to the office system. If the safety systems of the plant are completely isolated, does this mean that the extra virus protection is purely cosmetic - that is, security for security's sake? 'No, that's not true. The one thing that none of us in the nuclear industry can ever forget is that it is impossible to be *too* safe,' explains Hollick. 'Anything which makes the tools we use more reliable is always a good thing.'

Obviously there are lessons to be learned here for anyone responsible for running a mission-critical system. Firstly, if public alarm will result from a virus infection, this factor should be included in any risk assessment, and when deciding on security procedures. Secondly, the fact that *Nuclear Electric* made no effort to suppress the story acts in their favour: nothing looks worse than a bungled cover-up. Even in the nuclear industry, viruses are only a business problem. Having visited *Sizewell*, and seen their stringent security policies, it can be firmly stated that the *Sizewell B* 'incident' should be viewed in its true light: fiction, all too loosely based on fact.