Nuclear Plant Security and Cyber Terrorism

By Béla Lipták, PE, Columnist

During the last months, I wrote about the critical role that process control will play in converting our energy economy from an exhaustible to an inexhaustible one. In this series of articles, I will write about the role our profession will play during the transition when the planet seems to be drifting towards energy wars. The weapons of these wars of terror will not be limited to biological weapons and “dirty” nuclear bombs, but will also include software viruses and worms that will wage cyber warfare in attacking our infrastructure and industry, including our nuclear power plants.

My goal with this series of articles is not to spread fear, but to describe the power of process control to protect us. In order to illustrate my point, I selected the nuclear power industry to show how this can be done. I made that selection, because I want to deal with specific cases and nuclear power plants are convenient to illustrate the weak links that exist in this area.

Later I will describe the causes of such accidents as Three Miles Island or Chernobil. By the way, not too many people realize that some 11 Chernobil type nuclear power plant blocks are still in operation in Russia (at Kursk, Smolensk, Leningrad, etc.) and one is also operating until 2009 outside Russia (the Ignalina II block in Lituania). I will also discuss the causes of over 100 nuclear accidents of the past, plus the design and control configurations including interlocks that are used today and will describe the strategies by which process control can protect them from both the common accidents and cyber attacks.

While the targets of cyber attacks of the past also included other industrial targets, here I will concentrate on nuclear power plants and on their existing means of protection and on

---

1 These attacks might have a variety of causes and have already started. For example in April this year the cyber-infrastructure of Estonia and in August that of Georgia was successfully attacked, not by religious fanatics hiding in mountain caves, but (probably) by the sophisticated software engineers of Russia.

2 This protection is already needed because for example the Web site Al-finan.org already provides software for “Electronic Jihad Application” which can be used for attacking any Web site with DOS (denial of service) worms. The method by which DOS worms can enter control software is the same that can be used to shut down an airport or the electric grid of a nation.


4 For example in January, 2003 the SQL Slammer worm disrupted the operation of some 13,000 ATMs on the Bank of America network or in 2008 the Russians shut down the communication network of Georgia. The American government maintains a Cyber Terrorist Watch List, yet it has found that during the first half
the changes needed to close the existing security loopholes. I will discuss the safety needs of all three processing operations: enrichment, power generation and waste disposal.

<table>
<thead>
<tr>
<th>MINING AND ENRICHMENT</th>
<th>REACTOR OPERATION</th>
<th>WASTE STORAGE</th>
</tr>
</thead>
<tbody>
<tr>
<td>Zippe type centrifuge</td>
<td>Indirect, pressurized water reactor</td>
<td>Cask used for nuclear waste storage</td>
</tr>
</tbody>
</table>

*Figure 1: The three main process steps in the nuclear power cycle from mining to waste disposal*

The Slammer Worm\(^6\) Attack on the Davis-Besse Power Plant

...of 2008, only 1% of the cyber attacks came from sources on that list, while 35% originated elsewhere from within the United States.

\(^5\) There is over 2,000 tons of weapons grade highly enriched uranium in storage around the world and some of these are already supplying a black market. For example, in November 2007 a gang was arrested in Slovakia that was trafficking in uranium which could have been used to build dirty bombs (other such arrests been reported from Russia, Kazakhstan, China and Libya). 50 kg of 85% uranium is the minimum requirement for building a nuclear bomb. In addition to weapons grade waste, the spent fuel rods from regular reactors are also in temporary storage. The United States alone is storing some 30,000 tons of spent fuel rods and 380,000 m\(^3\) of high level radioactive waste. Because no permanent disposal method been found, the nuclear waste is stored in water basins or in steel casks by the individual nuclear power plants. In the USA, weapons grade plutonium from dismantling nuclear weapons is stored in casks outside Amarillo, Texas.

\(^6\) A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself there. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their replication has already consumed system resources, slowing or halting the operation of the system. They differ from viruses as viruses need a host file, make their presence known by presenting messages and take up computer memory leading to system crashes. Worms on the other hand exist inside of other files, often in Word or Excel documents and cause the entire document to travel from computer to computer as a worm. The Slammer Worm, also known as Sapphire and SQL Hell is the fastest computer worm yet in history. It infected more than 90% of vulnerable hosts within 10 minutes and reached its full scanning rate (of more than 55 million scans/second) in 3 minutes.
The grounds of Davis-Besse nuclear power plant in Ohio are patrolled by armed guards and are surrounded by a double row of tall fences which are monitored electronically, just as are all other nuclear power plants. Tall fences reduce the probability of somebody driving a truck full of explosives into the plant. Yet, all of my readers know that fences do not protect against computer crashes, armed guards do not protect against viruses and software worms.

On January 25, 2003 a Slammer worm penetrated the private computer network of Ohio's Davis-Besse nuclear power plant. The worm entered by first penetrating the unsecured network of a contractor and squirmed its way into the Davis-Besse corporate business network and because that network was connected to the plant’s network, but bypassed its firewall, it spread to the plant network.

The following sequence followed. At 4:00 PM the operators noticed the slowing of the plant network and at 4:50 PM the Safety Parameter Display System (SPDS) crashed. The SPDS monitors the operation of the coolant system, core temperature, radiation levels and other critical conditions. At 5:13 PM the Plant Process Computer (PPC) also crashed. Therefore, although the plant’s network was protected by a firewall, both the plant’s SPDS and PPC were disabled for about five hours. Fortunately at the time the plant was not in operation, because a hole in the reactor head was being repaired. Another reason why no harm was done is because the analog backups of the SPDS and the PPC could not be attacked by the worm.

We must remember that all our nuclear power plants are old and decades ago, the controls of all nuclear power plants were completely analog. There were no data highways and therefore the data transfer between the plants and corporate offices were secure from cyber attacks. Today, digital systems monitor the critical operating conditions (valve openings, pump status, temperatures, pressures, levels, radiation, loading, etc.) of most nuclear plants, while they are still controlled by analog controls.

Through a number of accidents we have learned that if an intruder worm tampers with the digital monitoring system (like in the case of Davis-Besse's SPDS and PPC), and if the operators are allowed to overrule the automatic safety interlocks, virus or worm attacks are possible. We have also learned that the design and practices of the operator of the Davis-Besse plant (FirstEnergy) were apparently NOT in violation of NRC’s cyber security regulations.

We also know that for financial reasons and because of management convenience, the whole nuclear industry is drifting towards installing completely digital controls to allow the remote operation of some plant functions. This trend could have disastrous consequences not only in newly built nuclear power plants, but also in refineries, chemical plants and throughout industry.
While in the above discussion I concentrated on the Davis-Besse accident, I should note that this one Slammer attack has much wider implications. After this nationwide attack the National Security Telecommunications Advisory Committee concluded that the American electric grid as a whole is controlled by a “Byzantine network riddled by security holes, including unsecured SCADA systems and by unprotected connections between plant and company business networks.”

**How To Improve Nuclear Power Plant Security**

In order to improve nuclear plant security it is essential to realize both the need for totally separating the corporate business networks from the plant networks and to realize that digital firewalls *do not* guarantee this separation. This separation must be absolute and software firewalls are not! Because the safety of the public is involved, the implementation of this separation cannot be left up to each plant owner or operator, but must be mandated by the NRC; otherwise the people living near nuclear power plants, (such as the residents of Long Island, N.Y.) can not feel safe.

Therefore, the NRC must totally forbid not only the remote operation of nuclear plants, but also the linking of plant operations networks with corporate LANs (local area networks). The convenience and cost savings associated with these corporate links cannot justify the risk they cause to the public. This also means that the NRC should require total separation between the corporate networks of utilities and the SCADA networks of the plants. These SCADA networks control the remote terminal units (RTUs) sprinkled throughout the plants, directly monitoring and/or controlling the operation of power plant equipment.

As I will be discussing in more detail in the coming articles, the steps to be taken to guarantee plant safety and security are not limited to providing digital separation. For example, one must also guarantee both the reliability of the data reaching the operators AND must protect the plant from operator errors, which can be unintended OR INTENTIONAL. The 21st-century interpretation of Murphy’s law says that it is just as possible for an operator to smuggle a bomb into the control room as it is to smuggle in a software package.

Therefore, the protection in nuclear power plants must be served by both redundancy and automation. In addition, the redundancy should not be a simple backup, but a triple-redundancy voting system implemented for both the hardware and the software of the plant. This means that in all nuclear power plants, all critical measurements and status indicators would be made by three accurate sensors, and the control system would act on the “majority view” which would *automatically* schedule the “disagreeing sensor” for maintenance and recalibration. The same would apply to all software packages including SCADA, SPDS, PPC, etc. networks in the plant. Similarly, in case of the digital systems and networks, as soon as one disagrees with the “majority view,” that one would be disabled and checked for virus or worm attacks.
In the area of protecting the plant from intentional or unintentional operator errors, I would provide hardwired interlocks on all critical safety systems and would configure the controls in such a way that the operators cannot bypass them or shut them down. In addition, I would set up a national review board that would not only train and check the background of operators, but would also arrange for the review of all existing process control loops in all 125 nuclear power plants to make sure that the conditions that have caused the over 100 accidents of the past are not still present in any of them.

In the area of nuclear waste management, we know that each reactor produces 20 tons of nuclear waste per year, and this waste is locally stored, usually in steel casks at temporary waste sites. These casks can be penetrated by regular weapons will release radioactive cesium gas. While these waste sites can be guarded 24 hours a day, the only safe solution would be to have a permanent waste repository. In the meanwhile, process control can much improve the security of these waste sites right now.

In addition to making the nuclear power plants more secure I would also require the NCR to use the tools of process control to improve the security of the uranium enrichment, transportation and waste storage (including military waste) in order to minimize the potential for theft. For obvious reasons, here I will not elaborate on the tools process control can provide to monitor and protect such sites, but just mention that it should be utilized if we want to protect societies around the globe from possible “dirty bomb” attacks.

I will continue this series in the January issue.

---

1 These attacks might have a variety of causes and have already started. For example in April this year the cyber-infrastructure of Estonia and in August that of Georgia was successfully attacked, not by religious fanatics hiding in mountain caves, but (probably) by the sophisticated software engineers of Russia.

2 This protection is already needed because for example the Web site Al-jinan.org already provides software for “Electronic Jihad Application” which can be used for attacking any Web site with DOS (denial of service) worms. The method by which DOS worms can enter control software is the same that can be used to shut down an airport or the electric grid of a nation.


4 For example in January, 2003 the SQL Slammer worm disrupted the operation of some 13,000 ATMs on the Bank of America network or in 2008 the Russians shut down the communication network of Georgia. The American government maintains a Cyber Terrorist Watch List, yet it has found that during the first half of 2008, only 1% of the cyber attacks came from sources on that list, while 35% originated elsewhere from within the United States.

5 There is over 2,000 tons of weapons grade highly enriched uranium in storage around the world and some of these are already supplying a black market. For example, in November 2007 a gang was arrested in Slovakia that was trafficking in uranium which could have been used to build dirty bombs (other such arrests been reported from Russia, Kazahstan, China and Lybia). 50 kg of 85% uranium is the minimum requirement for building a nuclear bomb. In addition to weapons grade waste, the spent fuel rods from regular reactors are also in temporary storage. The United States alone is storing some 30,000 tons of spent...
fuel rods and 380,000 m\textsuperscript{3} of high level radioactive waste. Because no permanent disposal method been found, the nuclear waste is stored in water basins or in steel casks by the individual nuclear power plants. In the USA, weapons grade plutonium from dismantling nuclear weapons is stored in casks outside Amarillo, Texas.

regular reactors are also in temporary storage. The United States alone is storing some 30,000 tons of spent fuel rods and 380,000 m\textsuperscript{3} of high level radioactive waste. Because no permanent disposal method been found, the nuclear waste is stored in water basins or in steel casks by the individual nuclear power plants. In the USA, weapons grade plutonium from dismantling nuclear weapons is stored in casks outside Amarillo, Texas.

6\textsuperscript{1} A worm is a self-replicating virus that does not alter files but resides in active memory and duplicates itself there. Worms use parts of an operating system that are automatic and usually invisible to the user. It is common for worms to be noticed only when their replication has already consumed system resources, slowing or halting the operation of the system. They differ from viruses as viruses need a host file, make their presence known by presenting messages and take up computer memory leading to system crashes. Worms on the other hand exist inside of other files, often in Word or Excel documents and cause the entire document to travel from computer to computer as a worm. The Slammer Worm, also known as Sapphire and SQL Hell is the fastest computer worm yet in history. It infected more than 90\% of vulnerable hosts within 10 minutes and reached its full scanning rate (of more than 55 million scans/second) in 3 minutes.

7\textsuperscript{1} This would include not only the operating plants, but also the 13 plants that have been shut down and the 10 plants that have been decommissioned.

8\textsuperscript{1} Past accidents included the partial meltdown at Three Miles Island caused by a failed relief valve and faulty level and temperature sensors, Chernobil caused by the disabling of the control computer ny the operators and a number of others including Chalk River, Canada, Windscale Pile, England, Greifswalld, Germany, Mihama, Tsuruga and Tokaimura in Japan, Areve, Tricastin, etc,France, Kystin, Russia and elsewhere.