Nuclear Power Plant Cyber-security Incidents

(extracts from Brent Kesler, "The vulnerability of nuclear facilities to cyber attack", Strategic Insights, Spring 2011

1. Davis Besse NPP, USA, Jan 2003

The Slammer worm infected computer systems at the Davis-Besse nuclear power plant, Ohio. The worm travelled from a consultant's network, to the corporate network of First Energy Nuclear, the licensee for Davis-Besse, then to the process control network for the plant. The traffic generated by the worm clogged the corporate and control networks. For four hours and fifty minutes, plant personnel could not access the Safety Parameter Display System (SPDS). Slammer did not affect analogue readouts; plant operators could therefore still get reliable data. Davis-Besse had a firewall protecting its corporate network from the wider internet, and its configuration would have prevented a Slammer infection. However, a consultant had created a connection behind the firewall to the consultancy's office network. This allowed Slammer to bypass the firewall and infect First Energy's corporate network. From there, it faced no obstacle on its way to the plant control network. In response, First Energy set up a firewall between the corporate network and the plant control network.

The Davis-Besse incident highlighted the fact that most nuclear power plants, by retrofitting their SCADA systems for remote monitoring from their corporate network, had unknowingly connected their control networks to the internet. At the time, the NRC did not permit remote operation of plant functions.

2. Browns Ferry NPP, USA, Aug 2006

The August 19, 2006, shutdown of Unit 3 at the Browns Ferry nuclear plant near Athens, Alabama, demonstrates that not just computers, but even critical reactor components, could be disrupted and disabled by a cyber attack. Unit 3 was manually shutdown after the failure of both reactor recirculation pumps and the condensate demineralizer controller. The condensate demineralizer used a programmable logic controller (PLC); the recirculation pumps depend on variable frequency drives (VFD) to modulate motor speed. Both kinds of devices have embedded microprocessors that can communicate data over the Ethernet LAN. However, both devices are prone to failure in high traffic environments. A device using Ethernet broadcasts data packets to every other device connected to the network. Receiving devices must examine each packet to determine which ones are addressed to them and to ignore those that are not. It appears the Browns Ferry control network produced more traffic than the PLC and VFD controllers could handle; it is also possible that the PLC malfunctioned and flooded the Ethernet with spurious traffic, disabling the VFD controllers; tests conducted after the incident were inconclusive. The failure of these controllers was not the result of a cyber attack. However, it demonstrates the effect that one component can have on an entire process control system network and every device on that network.

3. Hatch NPP, USA, March 2008

Due to the growing network connections between control systems and office computers, even seemingly simple actions can have unexpected results. On March 7, 2008, Unit 2 of the Hatch nuclear power plant near Baxley, Georgia, automatically shutdown after an engineer applied a software update to a single computer on the plant's business network. The computer was used to collect diagnostic data from the process control network; the update was designed to synchronize data on both networks. When the engineer rebooted the computer, the synchronization program reset the data on the control network. The control systems interpreted the reset as a sudden drop in the reactor's water reservoirs and initiated an automatic shutdown. This innocent mistake demonstrates how malicious hackers could make simple changes to a business network that end up affecting a nuclear reactor—even if they have no intent to interfere with critical systems. It also demonstrates that plant operators in this case did not fully understand the dependencies between network devices. This would make it difficult to identify and protect all the vulnerabilities in a process control system.