Supervisory control and data acquisition, other wise known as SCADA is a type of control system that uses the computers data in a network or graphical interface for process management. The system allows one central computer to control other coordinating computers and so on… this goes down to the field level.

There are many reasons why the federal government is afraid of SCADA attacks, one of the biggest ones, as stated by Capriz, is attacks on the grid. One of the main problems he stated is that most plants use a depreciation cycle of 5-25 years, this means that their equipment and technology can be old and use older versions of windows that are no longer covered by Microsoft.

Some of the main fears include tampering with or shutting down switches that regulate the flow of electricity (Capriz, 3). An attacker could open all the switches and then close them to cause a severe power outage. The switches themselves learn over time to reach maximum efficiency, but a little tampering could go almost undetected.

These types of attacked could wipe out a whole business’ infrastructure in a matter of seconds. The US Department of Energy has created policy suggestions to help prevent these types of attacks, but the problem is the price tag and the amount of time it takes to implement.

Sources:

Capriz, Marco. “SCADA Insecurity: The Most Worrying Cyber Attack.” Iuncturae, 18 Mar. 2017, www.iuncturae.eu/2017/03/18/scada-insecurity-the-most-worrying-cyber-attack/.